Authorized Send

Installation and Configuration Guide

for imageRUNNER Machines

Version 4.1

08011-41-UD2-003

This page is intentionally left blank.

Contents

This page is intentionally left blank.

Preface

Thank you for purchasing the Authorized Send software application. Please read this manual thoroughly before operating the product on your MEAP-enabled machine to familiarize yourself with its capabilities, and to make the most of its many functions. After reading this manual, store it in a safe place for future reference.

How to Use This Manual

This manual assumes that the reader has a good understanding of MEAP (Multifunctional Embedded Application Platform). This manual does not provide instructions for using or operating the Authorized Send application. For instructions on using the Authorized Send application, see the *Authorized Send User's Guide for imageRUNNER Machines.*

Symbols Used in This Manual

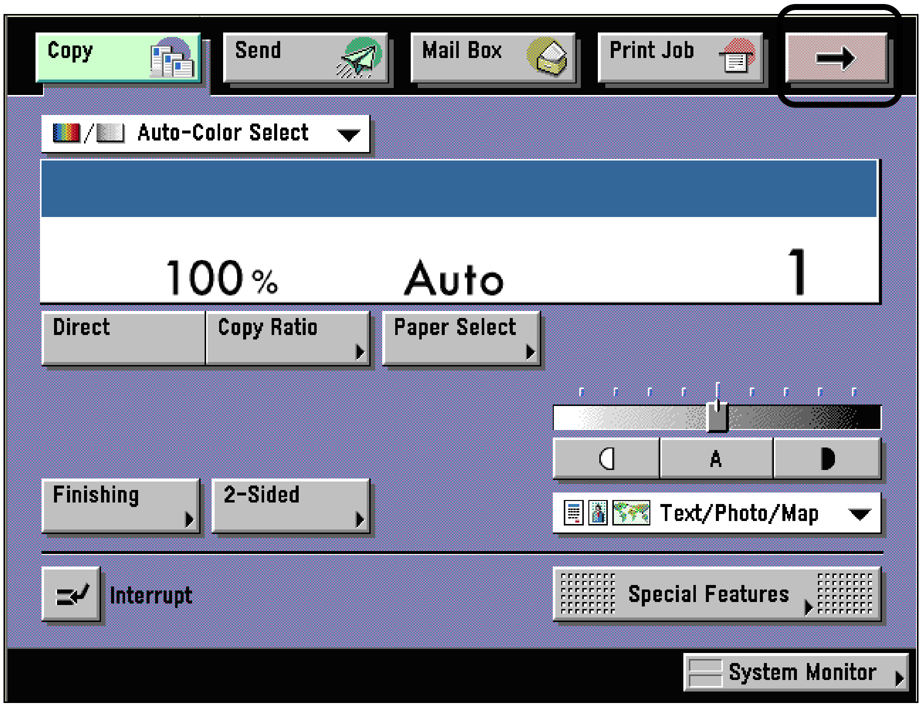
The following symbols are used in this manual to explain procedures, restrictions, and instructions that should be observed for safety.

IMPORTANT Indicates operational requirements and restrictions. Be sure to read these items carefully to operate the machine correctly, and avoid damaging the machine.

NOTE Indicates a clarification of an operation, or contains additional explanations for a procedure. Reading these notes is highly recommended.

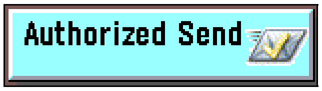
Keys and Buttons Used in This Manual

Keys for using the machine’s main functions are located on the top of the touch panel display. To use any of the desired function’s features, you must first press the key or application tab for the desired function. Press [→] (arrow key) to access installed MEAP applications.



On the MEAP Application screen, there may be several application tabs that you can select. Select only the proper tab for the application that you want to use.

The default application tab for Authorized Send is:



NOTE

The default tab name can be customized, and therefore the Authorized Send tab could have a different name.

The following key and button names are a few examples of how keys and buttons to be pressed and clicked are represented in this manual:

Touch Panel Display Keys:	[Key Name]
Examples:	[Scan]
	[Cancel]
Control Panel Keys:	Key Icon (Key Name)
Examples:	⊙ (Start)
	◈ (Stop)
Buttons on Computer Operations Screens:	[Key Name]
Examples:	[Install]
	[OK]

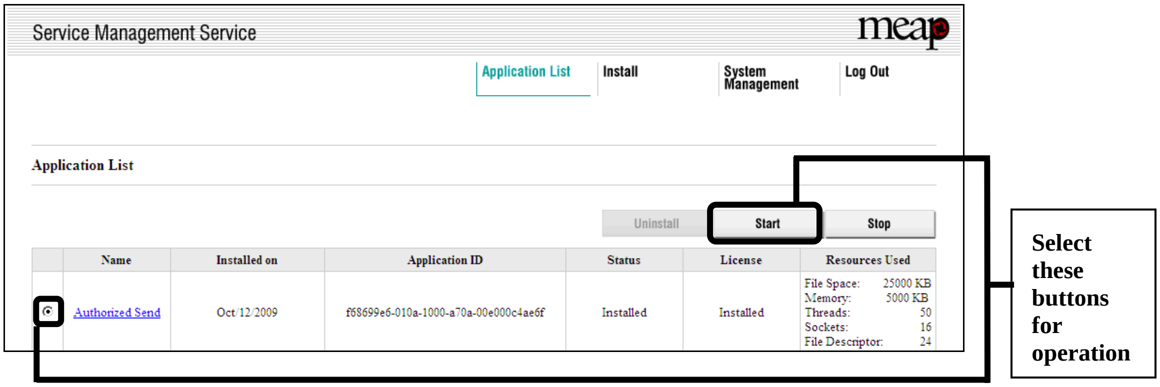
Displays Used in This Manual

Most screen shots used in this manual are those taken when Authorized Send is being installed using MEAP SMS (Service Management Service), or when Authorized Send is running on the Color imageRUNNER C5185, unless otherwise specified.

The keys/buttons you should select or click are marked with a circle, as shown below. When multiple keys/buttons can be selected on the screen, all keys/buttons are circled.

Example:

1. Select the [Authorized Send] radio button ➞ click [Start].



Application List

	Name	Installed on	Application ID	Status	License	Resources Used
⦿	Authorized Send	Oct/12/2009	f68699e6-010a-1000-a70a-00e000c4ae6f	Installed	Installed	File Space: 25000 KB Memory: 5000 KB Threads: 50 Sockets: 16 File Descriptor: 24

Select these buttons for operation

Abbreviations and Terms Used in This Manual

The following abbreviations are used in this manual.

Abbreviation	Definition
AD	Active Directory
ADF	Automatic Document Feeder
DFS	Distributed File System
DN	Distinguished Name
FQDN	Fully Qualified Domain Name
HID	Human Interface Device
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMS	License Management System
MEAP	Multifunctional Embedded Application Platform
MEAP device	Supported Canon imagePRESS, imageRUNNER, or Color imageRUNNER multifunctional machine featuring embedded MEAP technology.
NTLM	NT LAN Manager
Printable ASCII	These characters are from ' ' (space) up to and including '~' (tilde) on the ASCII table (the decimal values for the characters, x , are: 32 (space) ≤ x ≤ 126 (tilde)).
SMS	Service Management Service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
STRING	A set of consecutive characters that the user is able to input into a text box. If input into a text box is required, a string consisting of all spaces is not valid.
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator

Hyperlinks

When this manual is in its native PDF form, the blue underlined text represents a hyperlink to the corresponding sections of this manual or to external Web sites.

For example: See Chapter 1, "Overview," on p. 13.

Likewise, all entries in the Table of Contents are hyperlinks.

Legal Notices

Trademarks

Canon, the Canon logo, imageRUNNER, Color imageRUNNER, imagePRESS, and MEAP are registered trademarks, and the MEAP logo is a trademark, of Canon Inc. in the United States and may also be trademarks or registered trademarks in other countries.

Windows and .NET Framework are registered trademarks of Microsoft Corporation in the United States and are trademarks or registered trademarks of Microsoft Corporation in other countries.

Java and all Java-based trademarks and logos are the trademarks or registered trademarks of Sun Microsystems, Inc. in the United States or other countries.

Other product and company names herein are, or may be, the trademarks of their respective owners.

Copyright

Disclaimers

The information in this document is subject to change without notice.

CANON U.S.A., INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, EITHER EXPRESS OR IMPLIED, EXCEPT AS PROVIDED HEREIN, INCLUDING WITHOUT LIMITATION, THEREOF, WARRANTIES AS TO MARKETABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE OR NON-INFRINGEMENT. CANON U.S.A., INC. SHALL NOT BE LIABLE FOR ANY DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE, OR LOSSES OR EXPENSES RESULTING FROM THE USE OF THIS MATERIAL.

This page is intentionally left blank.

Chapter 1 Overview

Authorized Send is a customized MEAP application. It should be installed and operated on a Canon MEAP-enabled device, and provides authenticated scan to e-mail, scan to fax, and scan to folder functionalities. Authorized Send does not require the user to be authenticated to use the native functions of the machine, such as Copy, Print, and Scan, and does not interfere with any of these functions.

MEAP (Multifunctional Embedded Application Platform) is a software platform embedded in Canon imageRUNNER and imagePRESS machines that enables the development of custom applications, which run alongside native functions, such as Copy, Print, and Scan.

MEAP, developed by Canon, is based on Sun Microsystems' Java and Java 2 Micro Edition technology.

"MEAP device" is a MEAP-enabled Canon imageRUNNER or imagePRESS that is running the Authorized Send application. It may also be referred to as "MEAP imageRUNNER" or "machine."

imageRUNNER machines are the Canon imageRUNNERs, Color imageRUNNERs, and imagePRESS multifunctional machines.

Authorized Send is designed to perform the following functions once configured from the Authorized Send Configuration servlet:

- Authenticate against an LDAP server.
- Ability to disable LDAP authentication.
- Authenticate to an address book server anonymously.
- Retrieve a user's e-mail address and home directory.
- Search the LDAP address book server for e-mail addresses.
- Browse a network for valid share folders.
- Provide the ability to configure preset shares.
- Scan and send a document to a valid e-mail address, networked folder, or fax server.
- Enables a System Administrator to control the features that are available to a user.
- Enables a System Administrator to set default values for the Scan to E-Mail function.
- If activated, enables the use of the Searchable PDF, Encrypted PDF, and Compact PDF modes.
- Logs error and debugging information that is generated by the application to your local hard drive and to optional remote syslog servers.
- Scan in the PDF, TIFF, TIFF(Single), and JPEG file formats.
- Create folders that do not exist dynamically (in particular, using the user's User Name).

- Authenticate to a separate domain when scanning to a folder.
- Provide the ability to use NTLM Authentication for Scan to Folder, regardless of the authentication method used.
- Provide the ability to dynamically locate the closet available domain controller within the domain, and cache that domain controller until it becomes no longer available.
- Provide the ability to populate the User Name text box from a login application.
- Authenticate to a separate SMTP server.
- Job Build feature
- Ability to upgrade from previous versions of Authorized Send.
- MEAP Configuration Tool 1.0 compatibility.
- Ability to change the application display name.
- Ability to configure the application's images and colors.
- Ability to alter address book search results.
- Provide USB keyboard support.
- Enables a System Administrator to configure default scan settings for each file type.

IMPORTANT

- Basic knowledge of networking and imageRUNNER/imagePRESS machines is necessary to install and configure the Authorized Send application.
- For instructions on using Authorized Send, see the *Authorized Send User's Guide for imageRUNNER Machines.*
- The device must support MEAP Spec Version 13 to use the PDF Encryption feature.

1.1 System Requirements

Authorized Send requires the proper installation and configuration of all items documented in this guide. Failure to correctly install or configure the application will affect its operation.

If Authorized Send is not working properly, the problem can likely be traced to an installation or configuration issue. Please consult the appropriate chapters (including Chapter 5, "Troubleshooting," on p. 149) before contacting Canon U.S.A.'s e-Support.

1.1.1 Hardware Requirements

Authorized Send is designed to operate on the following Canon MEAP-enabled devices using the minimum specified MEAP Contents version.

Device Family	MEAP Contents
imageRUNNER 2270/2870/3570/4570	32.02
imageRUNNER 8070/9070/85+/105+	11.03
imageRUNNER 5570/5070/6570	35.02
imageRUNNER C3170	20.25
imageRUNNER 7105/7095/7086	35.02
imageRUNNER C6870/C5870	11.03
imageRUNNER C5180/C4580/C4080	20.05
imagePRESS C1	1.08
imageRUNNER C3380/C2880	10.02
imageRUNNER 3025/3030/3035/3045	10.05
imageRUNNER 5075/5065/5055	10.04
imageRUNNER C5185/C5180/C4580/C4080 (Version up)	65.13
imageRUNNER C3380/C2880 (Version up)	60.06
imagePRESS C7000VP/C6000VP/C6000	10.07
imageRUNNER C5058/C5068	60.13
imageRUNNER 5055/5065/5075 V2	30.04
imageRUNNER 5050	30.04
imageRUNNER 7086/7086N/7086B/7095/7095P/7105/7105B V2	55.03
imageRUNNER C2550/C3480	75.45
imageRUNNER 3225/3230/3235/3245	21.06
imagePRESS C1+	1.10

IMPORTANT

- MEAP and Use HTTP settings (from the Additional Functions screen) on the MEAP device must be enabled. (See the *Reference Guide* or the appropriate e-manual that came with your machine.)
- Access to System Manager Settings (from the Additional Functions screen) on the MEAP device is necessary.
- There must be network connectivity between the MEAP device, Active Directory servers, an e-mail server, and shared file servers.
- Inbox 99 on the MEAP device must be available for use, and without password protection.

1.1.2 Server Requirements

Authorized Send communicates with the following servers:

- Supported authentication servers:
  - Windows 2000 SP4/2003 SP2/2008 SP1 Active Directory
  - Lotus Domino Version 7
  - Novell NetWare 6.5/eDirectory 8.7 SP1 (or later)
- Supported address book servers:
  - Windows 2000 SP4/2003 SP2/2008 SP1 Active Directory
  - Lotus Domino Version 7
  - Novell NetWare 6.5/eDirectory 8.7 SP1 (or later)
- Supported name servers:
  - Windows 2000 SP4/2003 SP2/2008 SP1 (or later) DNS server
- Supported Scan to E-Mail servers:
  - Microsoft Exchange Server 2000/2003/2007 SP1
- Supported Scan to Network Share servers (with the exclusion of Cluster Server environment):
  - Windows Vista SP1/XP SP2/2000 SP4/2003 SP2 (or later)/2008 SP1 Local Share
  - Windows Vista SP1/XP SP2/2000 SP4/2003 SP2 (or later)/2008 SP1 Domain Share
  - Windows DFS (Distributed File System) Share
    - Windows Vista SP1/XP SP2/2000 SP4/2003 SP2/2008 SP1
- The following fax servers have been tested:
  - Relay Fax 6.7 by ALT-N Technologies
    (In order for the Scan to Fax function to work successfully with Relay Fax, each fax number used must have a corresponding e-mail address.)

1.1.3 Software Requirements

Microsoft Internet Explorer 6.0 or later, with JavaScript enabled, must be installed and configured prior to installing the Authorized Send application.

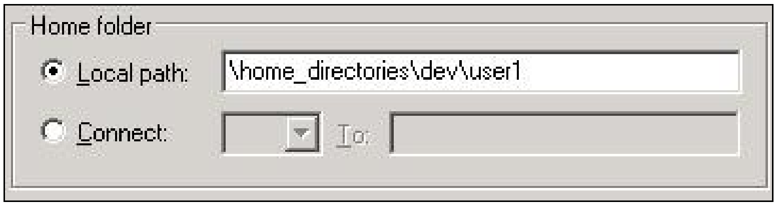
KDC is necessary for running Kerberos authentication.

1.1.4 Home Directory Requirements

If the System Administrator wants to configure the Retrieve Home Directory (Active Directory only) feature, the following three types of configurations are supported.

- **Local Share**

  This configuration illustrates when the home directory exists on the authentication server as a local share. No text manipulation is required, and the value entered is used exactly as is.



Home folder

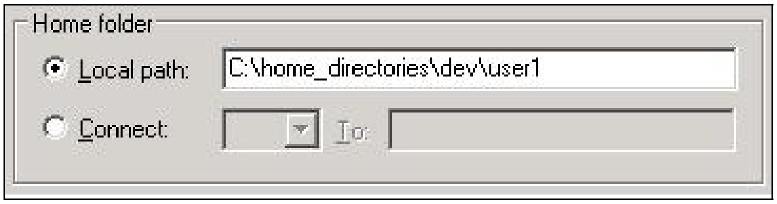
● Local path: \home_directories\dev\user1

○ Connect: To:

Home Directory as a Local Share

- **Local Path**

This configuration illustrates when the home directory exists on the authentication server as a local folder.



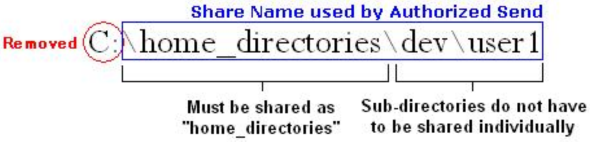
Home folder

● Local path: C:\home_directories\dev\user1

○ Connect: To:

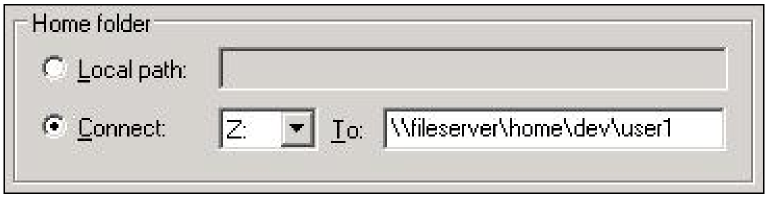
Home Directory as a Local Path

When the home directory exists on the authentication server as a local folder, it is impossible for Authorized Send to use the text as it is. Therefore, some text manipulation is required. In this case, Authorized Send removes the leading drive letter (in this case, “C:”), and then the rest of the text is treated as a local share. In this example, “home_directories” must be a valid share name.


Share Name used by Authorized Send
Removed
C:\home_directories\dev\user1
Must be shared as "home_directories"
Sub-directories do not have to be shared individually

- **Mapped Share**

This configuration illustrates when the home directory exists as a mapped share. In this example, “fileserver” is used as the host name of the file server, and “\home\dev\user1” is used as the share’s file path.



Home folder

○ Local path:

● Connect: Z: To: \\fileserver\home\dev\user1

Home Directory as a Mapped Share

1.1.5 Distributed File System Requirements

Authorized Send supports the following two DFS (Distributed File System) roots.

- **Stand-alone DFS root**
- **Domain-based DFS root**

  Successful domain-based DFS root support for Authorized Send requires that certain configuration settings be implemented and understood.

  1. End users can only access the domain-based DFS roots that belong to the domain against which they were authenticated.

  2. The authentication server created with Authorized Send's Configuration servlet must have the Domain Name configured to match the FQDN.

  IMPORTANT
  If the authentication server is configured with a NetBIOS domain name, access is granted to the application; however, you will not be able to access any domain-based DFS roots.

  3. Browsing for domain-based DFS roots are not supported. A preset share or home directory must be configured, or be manually entered in the share location.

  IMPORTANT
  If you configure a preset share for a domain-based DFS root, the file server must be configured with the FQDN of the Domain (i.e., If the domain name is "MyCompany.com," then the file server must be configured with the FQDN "MyCompany.com." The FQDN is not case-sensitive.). This results in the domain-based DFS root's preset share on the file server matching the authentication server's domain name.

  4. The first successful DFS target is used; otherwise, the end user will not be able to scan to the DFS root.

1.1.6 Communication Interfaces

The table below shows the different communication interfaces, their specific port numbers, and descriptions used with Authorized Send.

Communication Interface	Port	Description
NTLM	Determined by AD server	Used for authentication.
Kerberos	UDP/TCP Port 88	Used for authentication.
LDAP	TCP Port 389	Used to retrieve e-mail addresses.
SMB	TCP Port 139 and TCP Port 445	Used for the Scan to Folder function.
SMTP	TCP Port 25	Used for the Scan to E-Mail function.
HTTP	TCP Port 8000	Used to access the administration Web page.
HTTPS	TCP Port 8443	Used to access the secure administration Web page.
SSL	TCP Port 636	Used to communicate with the LDAP server.
Syslog	UDP Port 514	Used to communicate with the syslog server.

1.1.7 Supported Authentication Protocols

Kerberos and NTLM are the supported protocols when communicating with a Microsoft Active Directory server.

Simple Binding is the supported protocol when communicating with Novell eDirectory and Lotus Domino.

Anonymous Binding is the protocol reserved for communication with any of the supported address book servers (when applicable).

IMPORTANT

If Simple is selected as the authentication method and Novell eDirectory is the targeted authentication server, set the following settings on the eDirectory server:

- Disable “Require TLS for Simple Binds with Password” for the LDAP Group.
- Disable “Require TLS for all operations” for the LDAP Server in the Connections section.
- In the Restrictions section, select [Use Low Cipher (56 or 64-bit)].

1.1.8 MEAP Application Coexistence Support

Authorized Send can coexist with other installed MEAP applications that have received verification by Canon U.S.A., Inc., provided that there are sufficient resources available on the MEAP device.

The following table shows the maximum values for MEAP resources that Authorized Send could use in a MEAP device.

MEAP Device Resource Requirements	Maximum
File space usage	25,000 KB
Memory usage	5,000 KB
File descriptor usage	20
Socket usage	16
Thread usage	50

Authorized Send has been confirmed to coexist with the following applications:

- Scan to Database 1.1
- Pharos 2.3.10 with Uniprint 8.0 (Not supported when the [Enable USB Keyboard input] check box on the Options screen is selected.)

1.2 Communication Environment

Authorized Send must be installed on a MEAP-enabled device. There must be network connectivity between the MEAP device, DNS, authentication servers, address book servers, SMTP server, and shared file servers.

It is necessary to configure Authorized Send to communicate with the authentication servers and address book servers.

The following table lists the supported authentication servers and authentication methods.

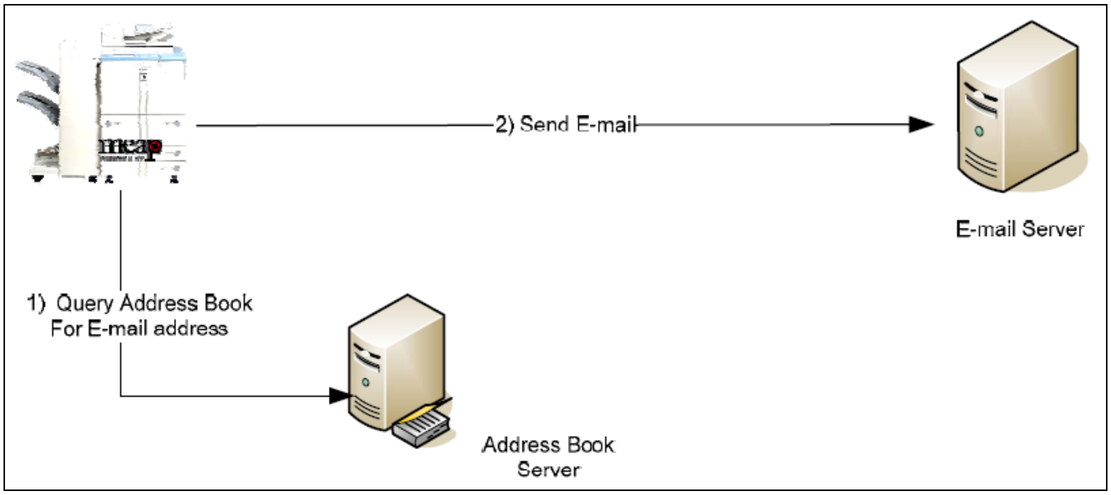
Supported Authentication Servers	Authentication Methods
Windows Active Directory	NTLM, Kerberos (with or without SSL)
Novell NetWare 6.5/eDirectory 8.7 SP1	Simple LDAP (with or without SSL)
Lotus Domino v7	Simple LDAP (with or without SSL)

The following table lists the supported address book servers and binding methods.

Supported Address Book Servers	Binding Methods
Windows Active Directory	NTLM, Kerberos (with or without SSL)
Novell NetWare 6.5/eDirectory 8.7 SP1	Simple LDAP (with or without SSL)
Lotus Domino v7	Simple LDAP (with or without SSL)

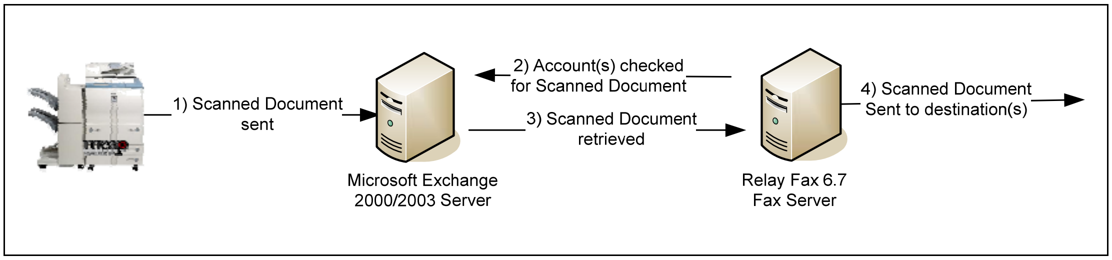
The following illustrations represent a flow of operations for the Scan to E-Mail, Scan to Fax, and Scan to Folder functions of the Authorized Send application.

Scan to E-Mail



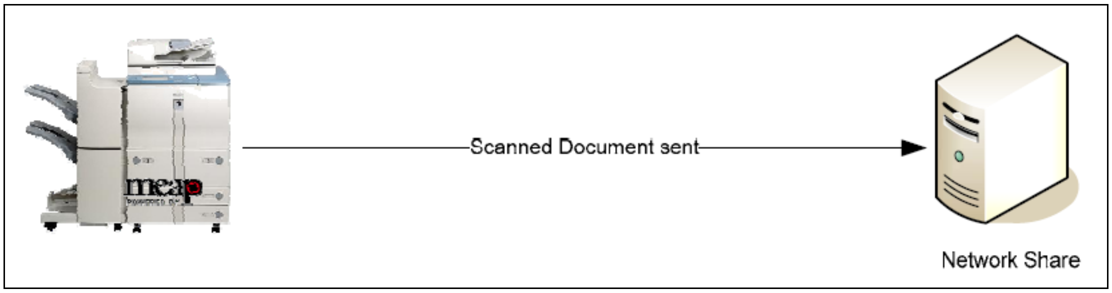
1. The user makes an address book query from the Scan to E-Mail function on the MEAP machine. The machine sends an LDAP query to the address book server to retrieve the desired list of e-mail addresses.
2. Once all e-mail addresses are verified and selected, the machine sends the e-mail message to the E-mail or SMTP server.

Scan to Fax



1. The user manually inputs the recipient’s fax number.
2. The machine sends the scanned document to the SMTP server.
3. The SMTP server sends the scanned document to the fax server.
4. The fax server sends the scanned document to the destination.

Scan to Folder

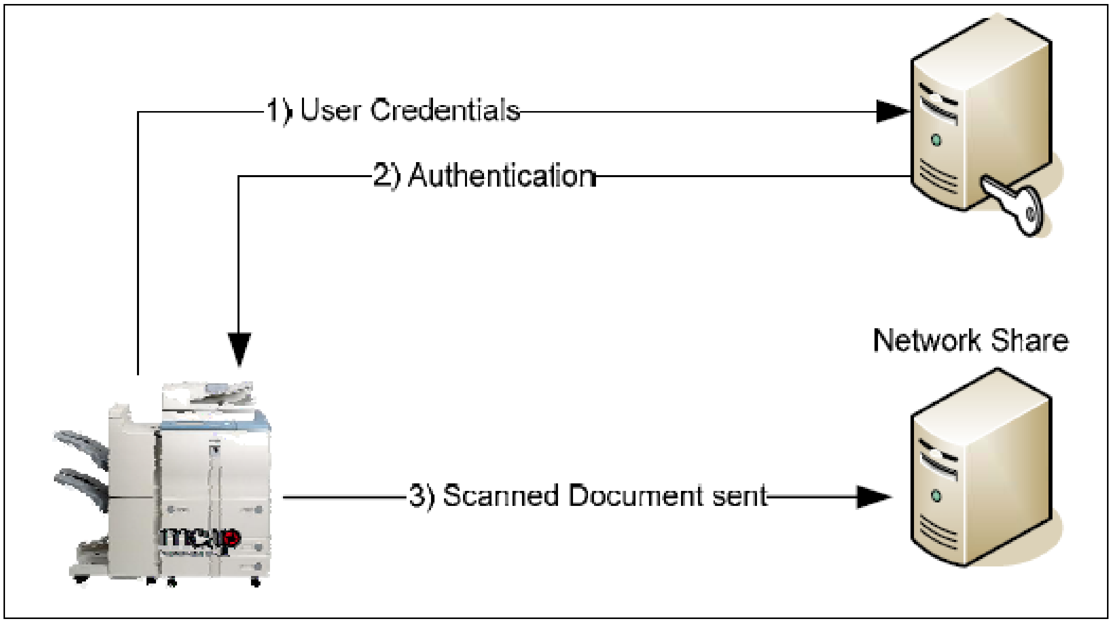


1. The user browses for the desired folder on the file server directly from the machine.
2. Once the directory is found and selected, the machine sends the file to the designated location on the file server.

✎ NOTE

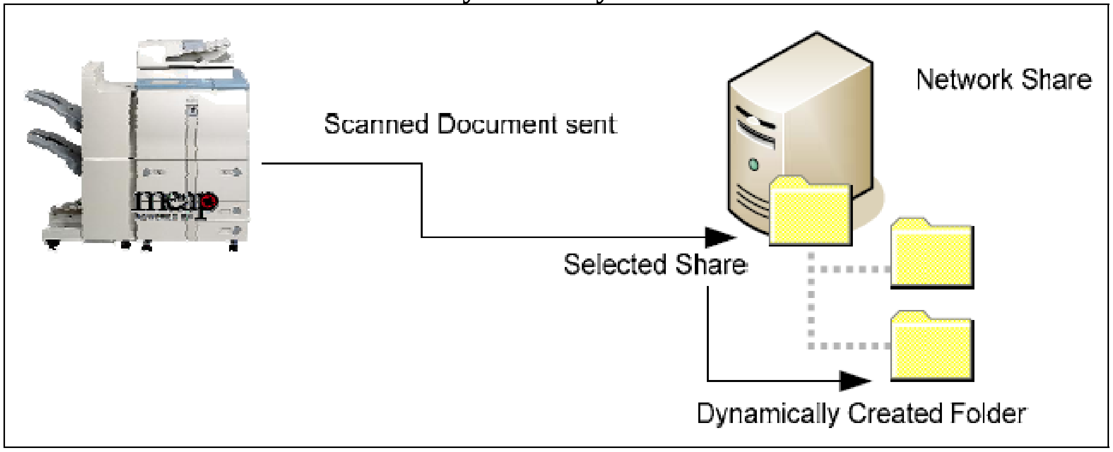
When a user accesses a network share, they are authenticated against that share using their credentials. If they do not have access rights to that share, they will be prompted to enter a user name and password.

Scan to Folder with NTLM Authentication



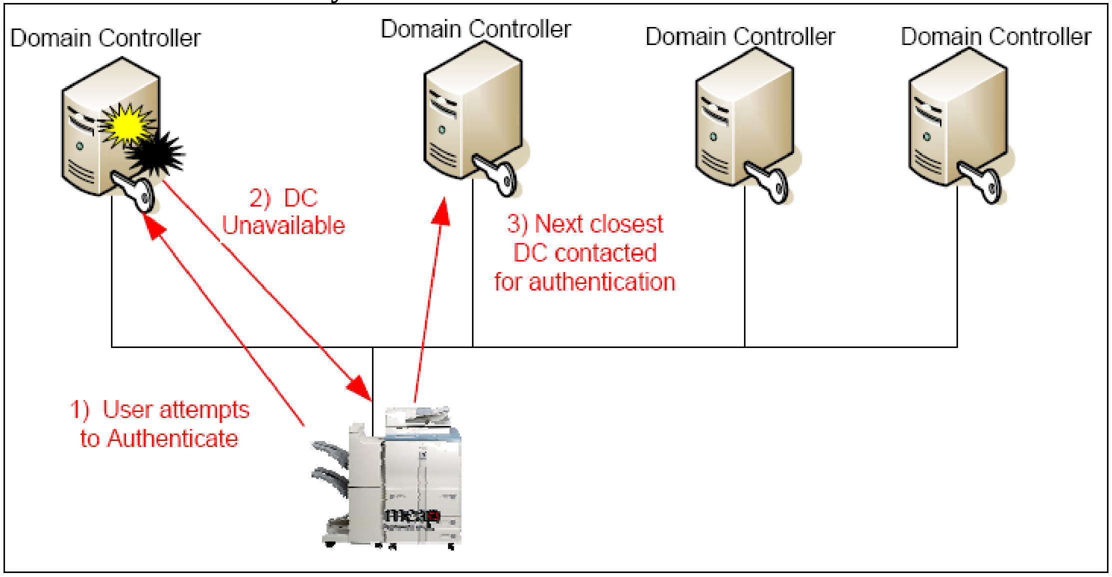
1. The user logs on to the machine using one of the authentication methods.
2. The user browses and enters their credentials to gain access to a network shared folder using NTLM as the authentication method.
3. Once access is granted, the scanned document is stored in the selected folder.

Scan to a Dynamically Created Folder



1. The authenticated user selects a folder, enters a document name, and scans the document.
2. The scanned document is automatically stored in a sub-folder (that was dynamically created) of the selected folder.

Dynamic Domain Controller Location



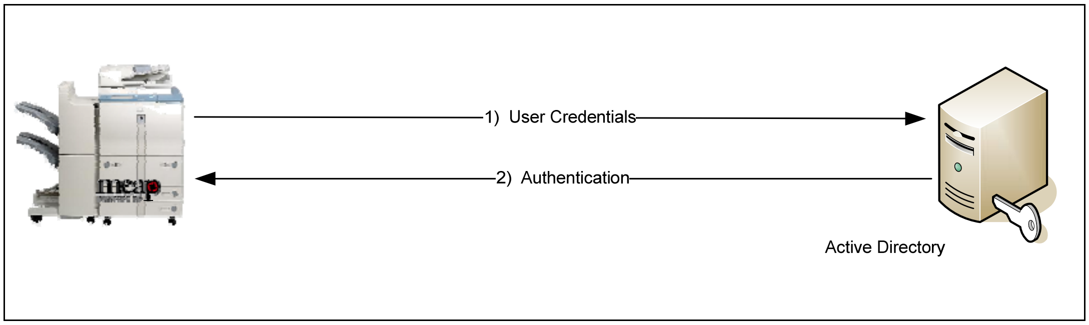
1. The user tries to log on to the machine using one of the authentication methods.
2. The system is unable to contact the authentication server previously cached.
3. The system locates the next closest available domain controller.
4. Authentication or address book lookup is performed by the new domain controller.
5. The new domain controller is cached.

1.2.1 Communication Diagrams

This section shows the flow of communication protocols based on the authentication method that you select. You can configure up to 10 authentication servers.

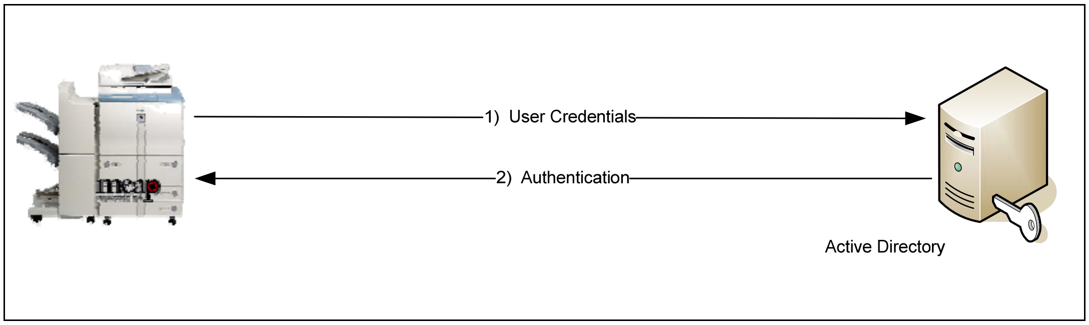
1.2.1.1 Authentication Communication Diagrams

Kerberos Authentication



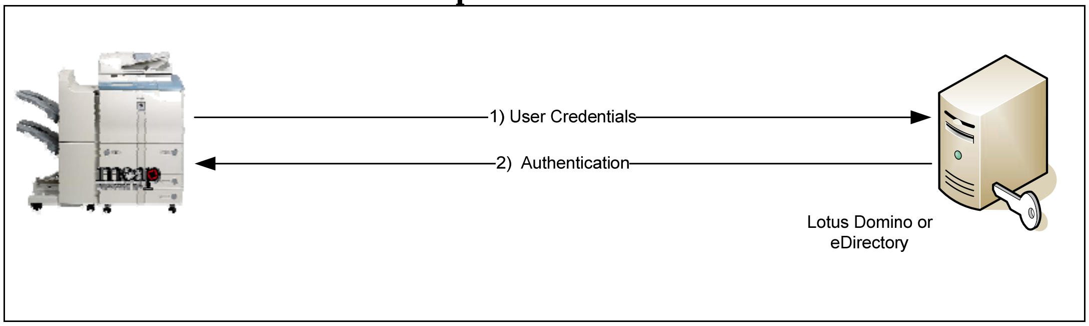
Communication Protocol LDAP/Kerberos

NTLM Authentication



Communication Protocol LDAP/NTLM

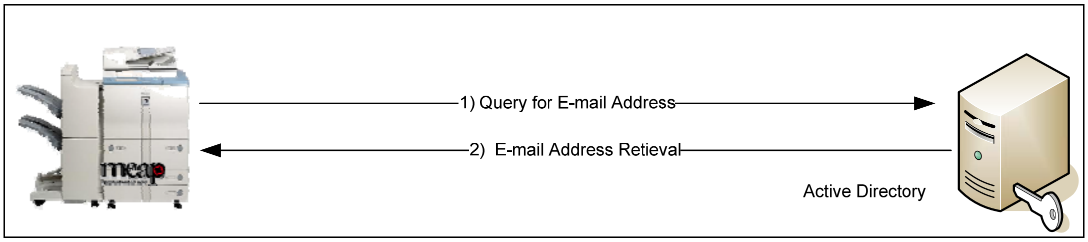
Simple Authentication



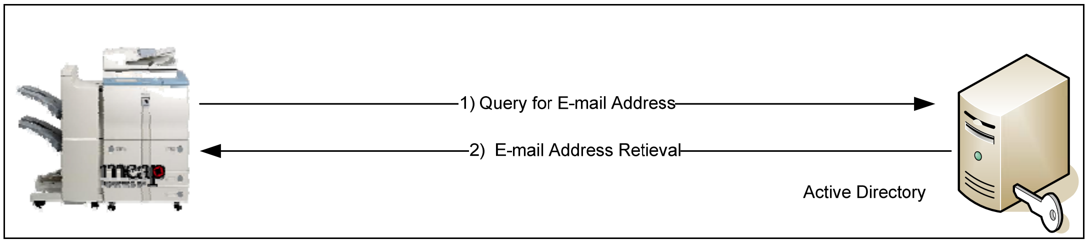
Communication Protocol LDAP/Simple

1.2.1.2 Address Book Communication Diagrams

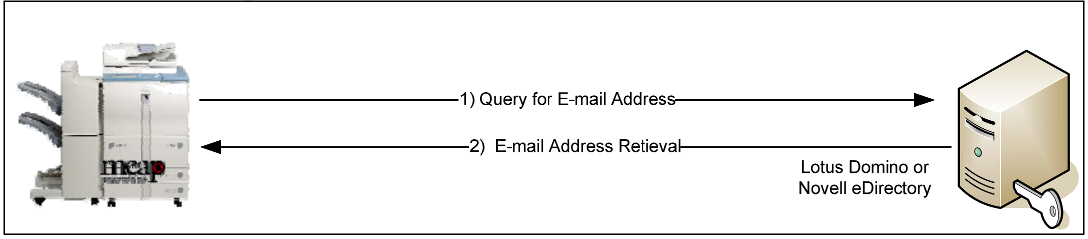
Kerberos Communication with an Address Book Server



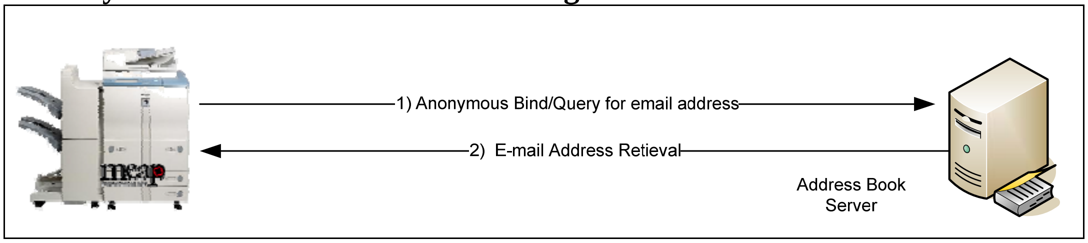
NTLM Communication with an Address Book Server



Simple Communication with an Address Book Server



Anonymous Bind Communication Using LDAP with an Address Book Server


1) Anonymous Bind/Query for email address
2) E-mail Address Retieval
Address Book
Server

This page is intentionally left blank.

Chapter 2 Installing Authorized Send

This chapter describes how to install Authorized Send on a MEAP-enabled machine using the MEAP SMS program.

The System Administrator for the target MEAP device is best suited for installing the Authorized Send application, using a networked computer that is connected to the Internet and the device.

Before installation, you must obtain the license file from www.canon.com/Meap, and have the IP address of the MEAP-enabled device.

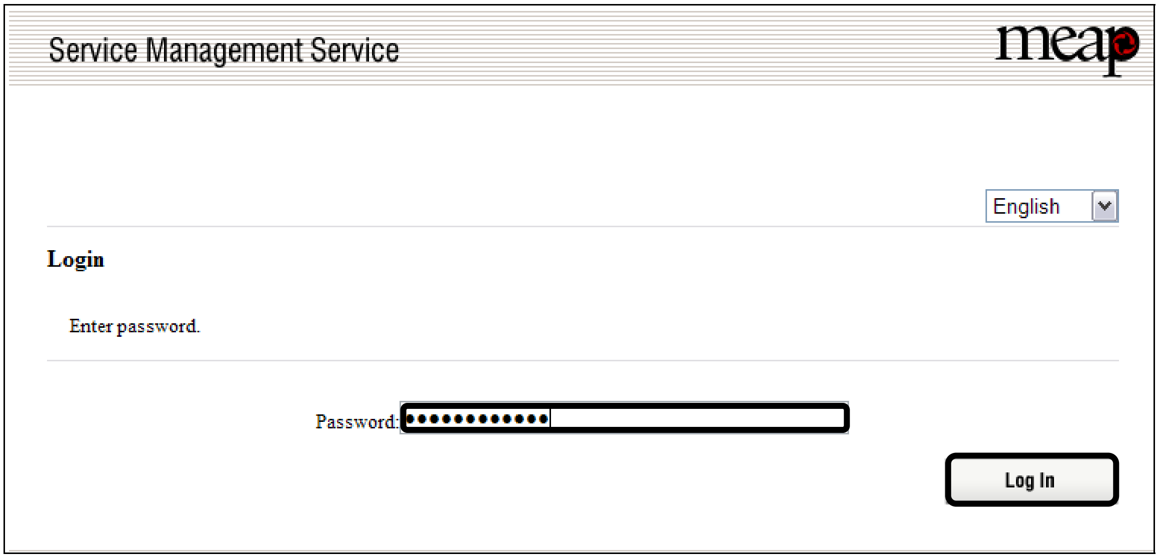
IMPORTANT

- This chapter describes the procedure for a new installation of Authorized Send Version 4.1.
- If you want to upgrade from a previous version of Authorized Send, you must uninstall the previous version from the MEAP device before installing this version. If you are upgrading from version 3.0, 3.51, 3.52, or 4.0 you do not have to uninstall the previous version if you are using the same license file (although you still must [Stop] the program).
- Do not use the browser's [Back] and [Forward] buttons during the installation process. Only use the clickable links in the browser's window.
- For more information on using SMS and uninstalling MEAP applications, see the *MEAP SMS Administrator Guide* that came with your MEAP device.

1. Open a browser window ➞ enter the following URL:

   http://<device IP>:8000/sms
   https://<device IP>:8443/sms (if you are using SSL for communications)
   (Replace <device IP> with the IP address of the MEAP device.)

2. Enter **MeapSmsLogin** in [Password] ➞ click [Log In].



Service Management Service

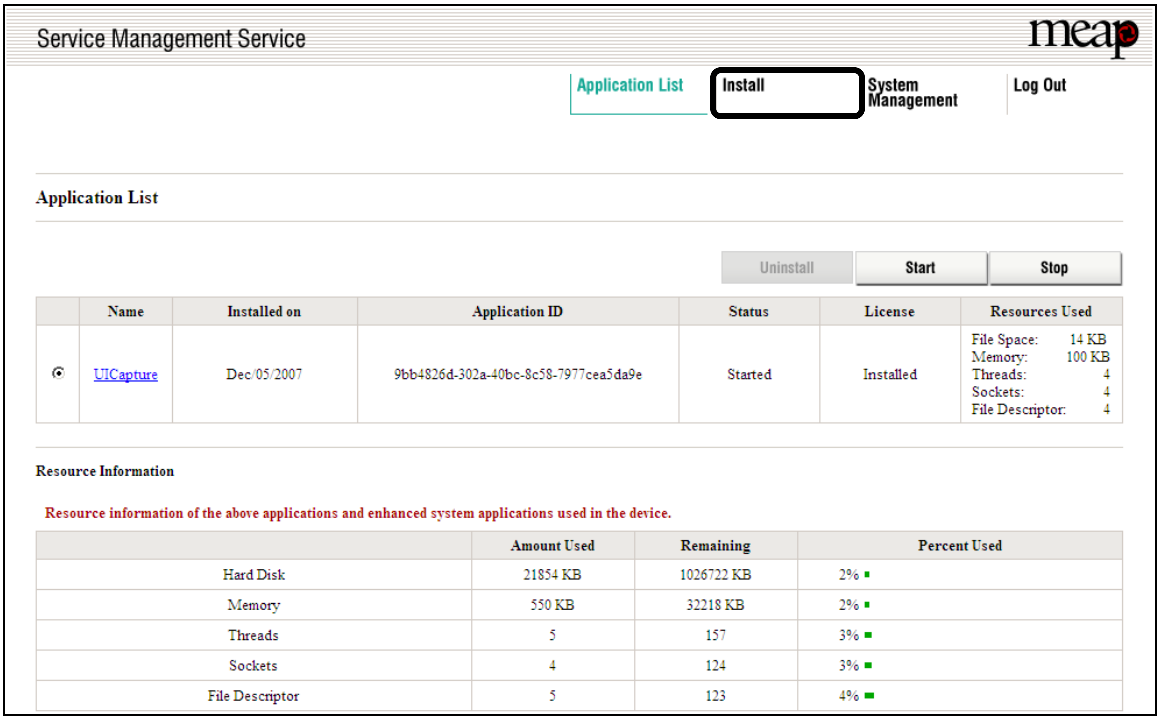
Login

Enter password.

Password: ●●●●●●●●●●●●

The SMS Application List screen is displayed.

3. Click the [Install] tab.



Service Management Service

Application List

	Name	Installed on	Application ID	Status	License	Resources Used
●	UICapture	Dec/05/2007	9bb4826d-302a-40bc-8c58-7977cea5da9e	Started	Installed	File Space: 14 KB Memory: 100 KB Threads: 4 Sockets: 4 File Descriptor: 4

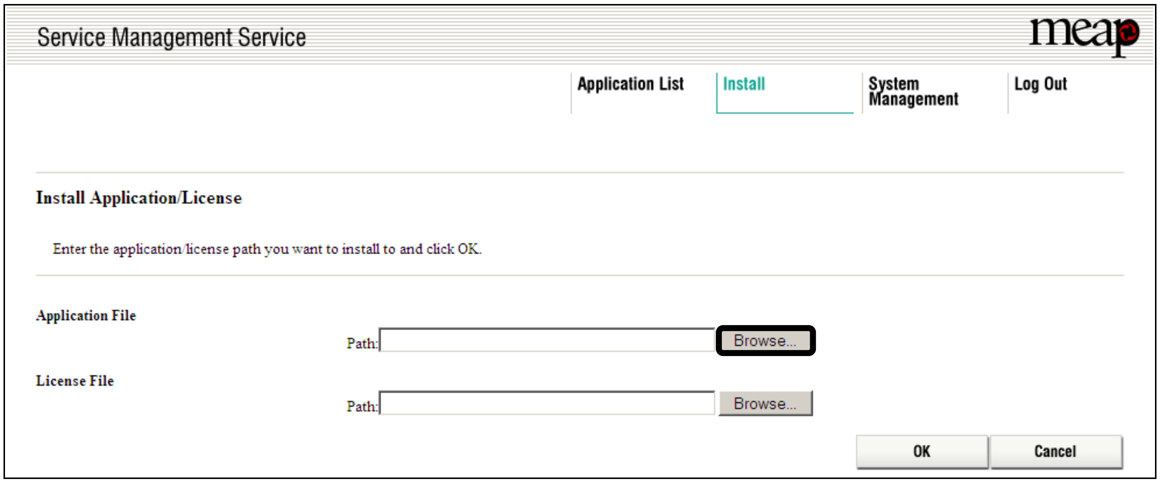
Resource Information

Resource information of the above applications and enhanced system applications used in the device.

	Amount Used	Remaining	Percent Used
Hard Disk	21854 KB	1026722 KB	2% ■
Memory	550 KB	32218 KB	2% ■
Threads	5	157	3% ■
Sockets	4	124	3% ■
File Descriptor	5	123	4% ■

The SMS Install Application/License screen is displayed.

4. Under <Application File>, click [Browse] to the right of Path.



Install Application/License

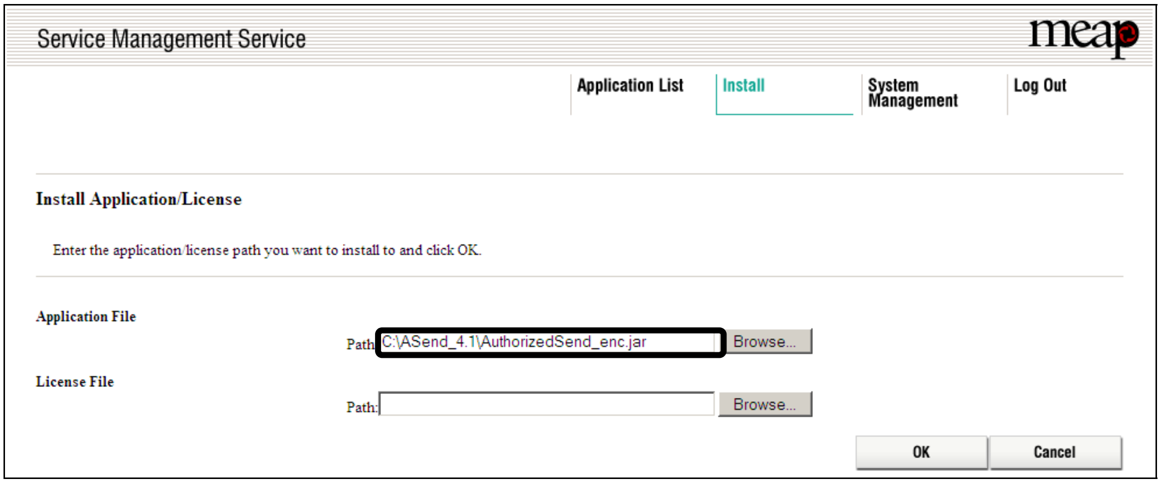
Enter the application/license path you want to install to and click OK.

5. Navigate to the drive or directory containing the .jar file ➞ select the file ➞ click [Open].

IMPORTANT

Make sure that you select the file that ends with the .jar extension for the application file.

6. Verify that the correct file was selected.



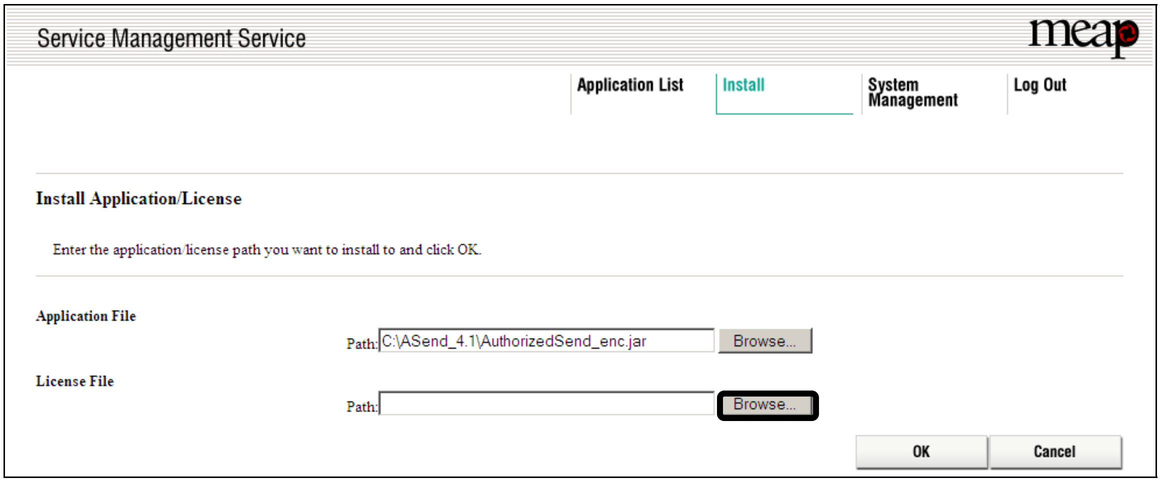
Install Application/License

Enter the application/license path you want to install to and click OK.

Application File

Path: C:\ASend_4.1\AuthorizedSend_enc.jar

7. Under <License File>, click [Browse] to the right of Path.



Install Application/License

Enter the application/license path you want to install to and click OK.

Application File

Path: C:\ASend_4.1\AuthorizedSend_enc.jar

License File

Path:

IMPORTANT

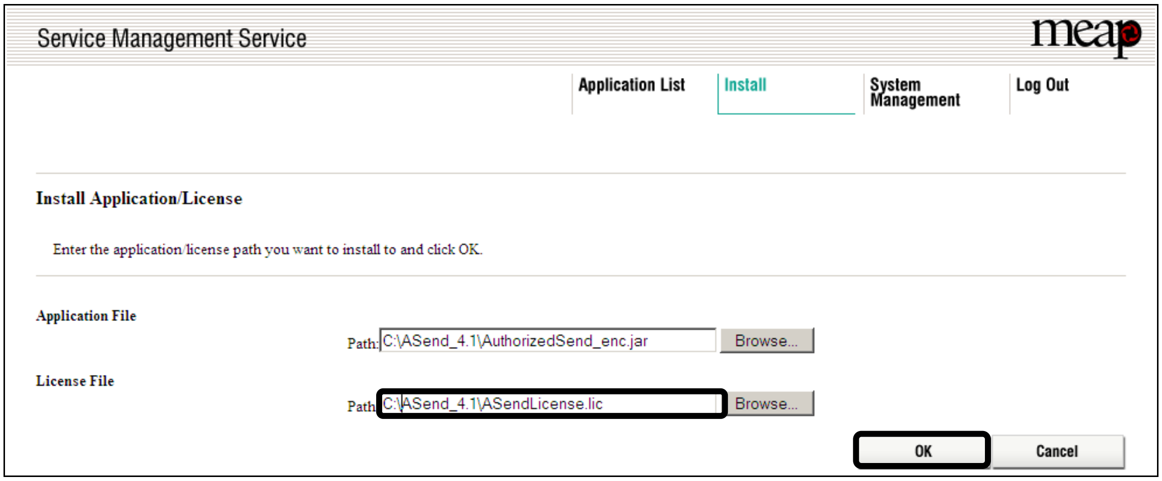
The license file must be downloaded from the LMS beforehand. For more information, contact your local authorized Canon dealer.

8. Navigate to the drive or directory containing the .lic file ➞ select the file ➞ click [Open].

IMPORTANT

Make sure that you select the file that ends with the .lic extension for the license file.

9. Verify that the correct file was selected ➞ click [OK].



Install Application/License

Enter the application/license path you want to install to and click OK.

Application File

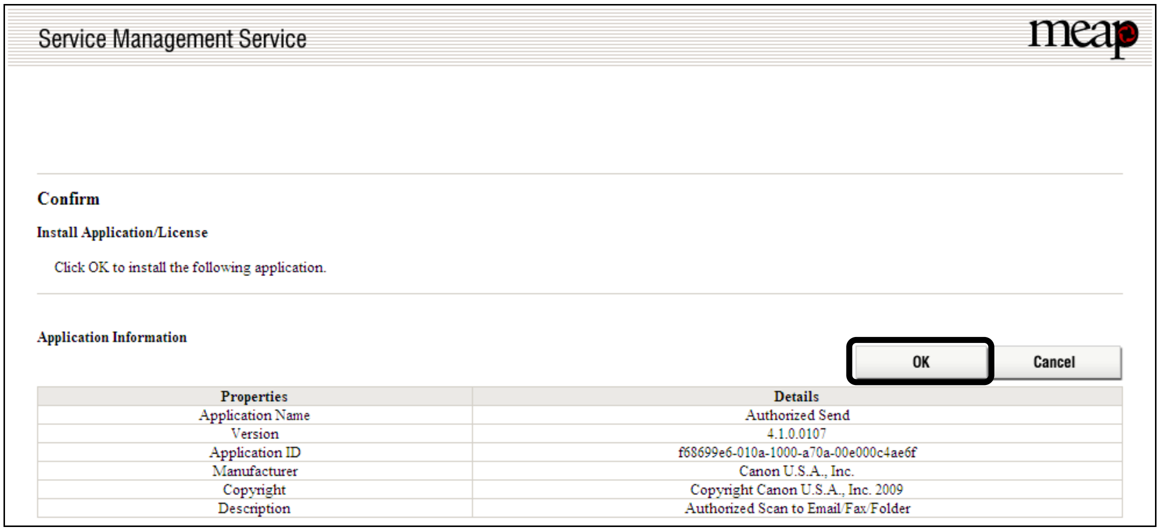
Path: C:\ASend_4.1\AuthorizedSend_enc.jar

License File

Path: C:\ASend_4.1\ASendLicense.lic

The SMS Confirm Install Application/License screen is displayed.

10. Click [OK].



Confirm

Install Application/License

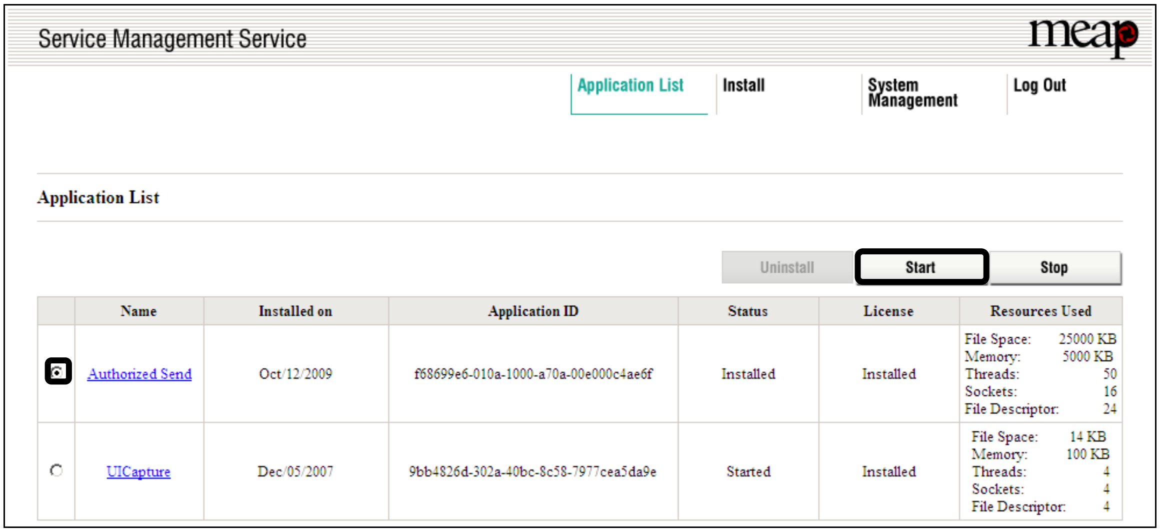
Click OK to install the following application.

Application Information

Properties	Details
Application Name	Authorized Send
Version	4.1.0.0107
Application ID	f68699e6-010a-1000-a70a-00e000c4ae6f
Manufacturer	Canon U.S.A., Inc.
Copyright	Copyright Canon U.S.A., Inc. 2009
Description	Authorized Scan to Email/Fax/Folder

During installation, the message <Installing…Please wait a moment.> is displayed.

11. Click the [Authorized Send] radio button ➞ click [Start].

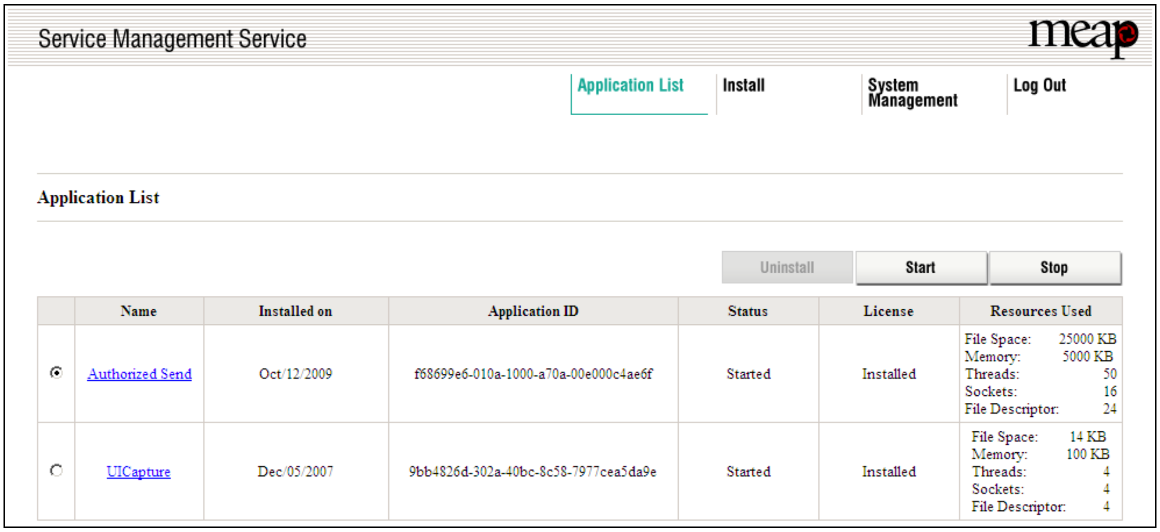


Application List

	Name	Installed on	Application ID	Status	License	Resources Used
●	Authorized Send	Oct/12/2009	f68699e6-010a-1000-a70a-00e000c4ae6f	Installed	Installed	File Space: 25000 KB Memory: 5000 KB Threads: 50 Sockets: 16 File Descriptor: 24
○	UICapture	Dec/05/2007	9bb4826d-302a-40bc-8c58-7977cea5da9e	Started	Installed	File Space: 14 KB Memory: 100 KB Threads: 4 Sockets: 4 File Descriptor: 4

Note that the status of the Authorized Send application is <Installed> before clicking [Start].

The status will change to <Started> if successful.



Application List

	Name	Installed on	Application ID	Status	License	Resources Used
●	Authorized Send	Oct/12/2009	f68699e6-010a-1000-a70a-00e000c4ae6f	Started	Installed	File Space: 25000 KB Memory: 5000 KB Threads: 50 Sockets: 16 File Descriptor: 24
○	UICapture	Dec/05/2007	9bb4826d-302a-40bc-8c58-7977cea5da9e	Started	Installed	File Space: 14 KB Memory: 100 KB Threads: 4 Sockets: 4 File Descriptor: 4

Installation is complete.

12. Click [Log Out] to exit SMS.

Chapter 3 Configuring Authorized Send

This chapter describes how to configure Authorized Send from a Web browser and set up the authentication servers, address book servers, share names, and options for the Scan to E-Mail, Scan to Fax, and Scan to Folder functions. It also describes how to configure the application's interface appearance using the optional Brand Configuration Tool.

The Authorized Send Configuration page contains the following items for configuring Authorized Send:

Authentication:	Create up to 10 authentication servers.
E-Mail Service:	
General:	Configure an SMTP server.
Address Book:	Configure up to 10 address book servers.
Scan to E-Mail:	Configure the Scan to E-Mail settings.
Scan to Fax:	Configure the Scan to Fax Settings.
Scan to Folder:	
General:	Configure the Scan to Folder settings.
Preset Shares:	Create preset folders for users to scan to.
Options:	Configure the optional settings.
Logs:	Configure the log settings, remote syslog servers, and download and view the logs.
About:	Display the Authorized Send version information.

3.1 Flow of Configuration Operations

From the Authorized Send Configuration screen, you can configure the settings necessary to use the Authorized Send application.

1. Open a browser window ➞ enter the following URL:

   http://<device IP>:8000/AuthSendConfiguration
   (Replace <device IP> with the IP address of the MEAP device.)

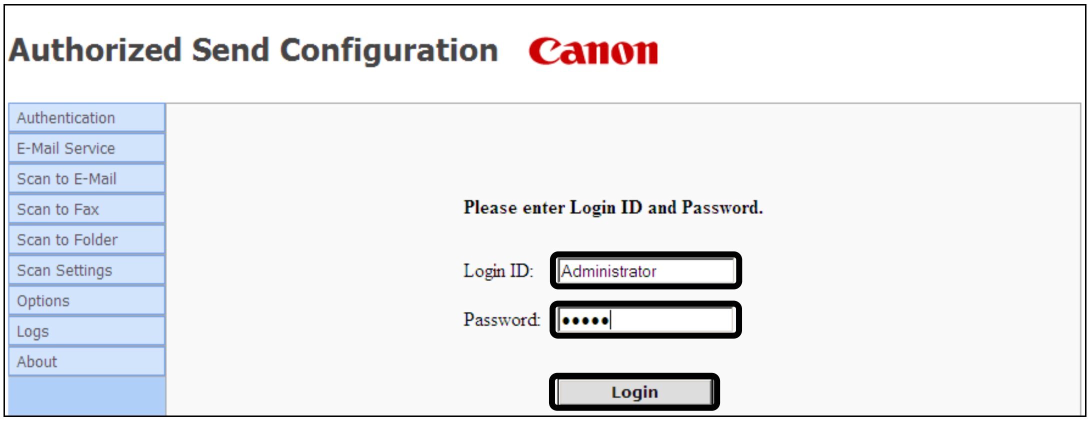
   The Please enter Login ID and Password screen is displayed.

IMPORTANT

- Enter **AuthSendConfiguration** exactly as shown, as it is case-sensitive.
- If Portal Service is installed, you can also access the Authorized Send Configuration screen by entering **http://<device IP>:8000** ➞ click the Authorized Send Configuration link. (Replace <device IP> with the IP address of the MEAP device.)

2. Enter your user name in [Login ID] and your password in [Password] ➞ click [Login].

   The default Login ID is ‘Administrator’, and the default password is ‘Admin’.



Please enter Login ID and Password.

Login ID: Administrator

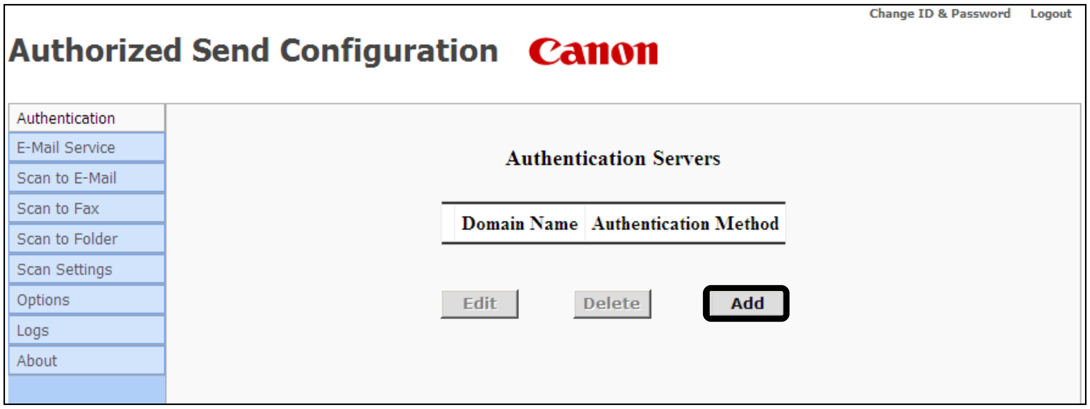
Password: •••••

   The Authentication Servers screen is displayed.

IMPORTANT

If you are using a temporary license and the license has expired, the message <The Authorized Send license has expired. Please contact your Canon dealer.> will be displayed. You must update your license file, or you will not be able to access the Configuration servlet.

3. Click [Add].



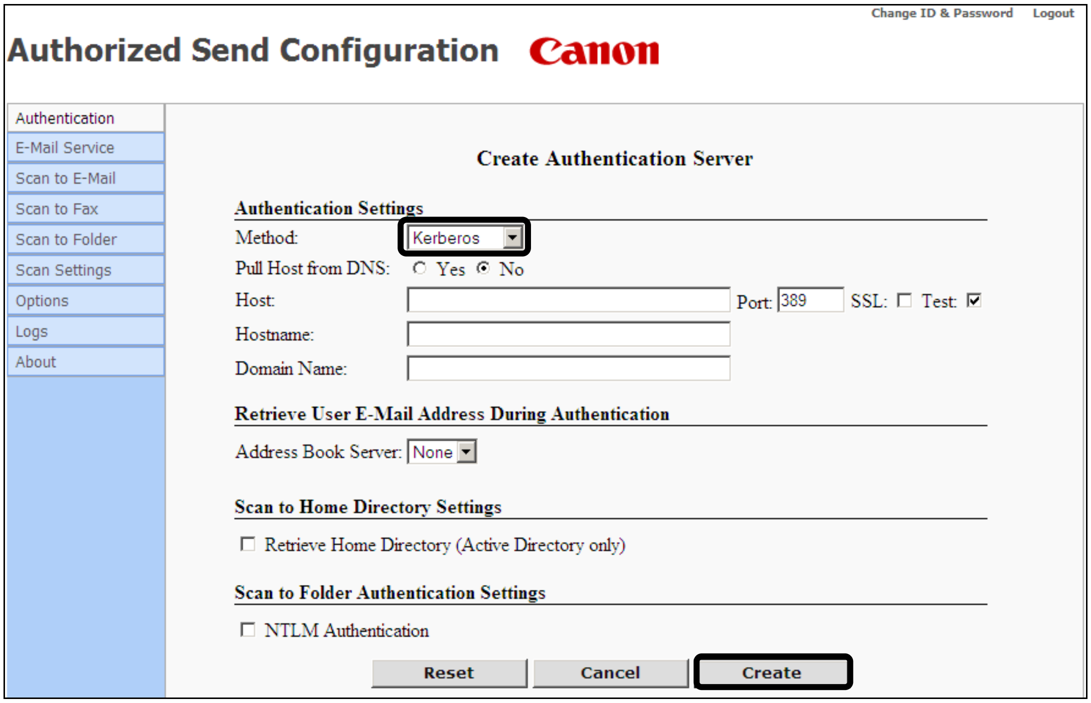
Authentication Servers

Domain Name	Authentication Method

   The Create Authentication Server screen is displayed.

4. Select the authentication method ➞ configure the settings based on the selected authentication method ➞ click [Create]. (See "Creating an Authentication Server," on p. 49.)

   The available settings vary, depending on the selected authentication method.



Create Authentication Server

Authentication Settings

Method: Kerberos

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test: ☑

Hostname:

Domain Name:

Retrieve User E-Mail Address During Authentication

Address Book Server: None

Scan to Home Directory Settings

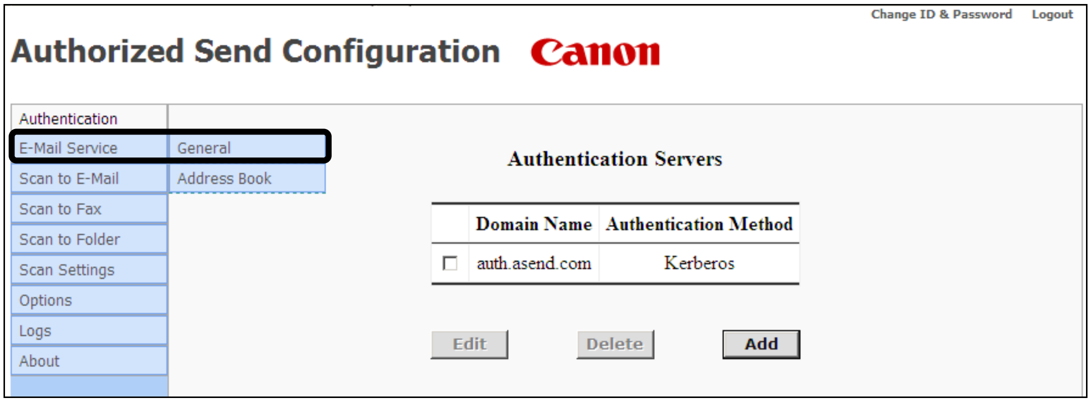
□ Retrieve Home Directory (Active Directory only)

Scan to Folder Authentication Settings

□ NTLM Authentication

   The Authentication Server is created, and is added to the list on the Authentication Servers screen.

5. Click [E-Mail Service] ➞ [General].

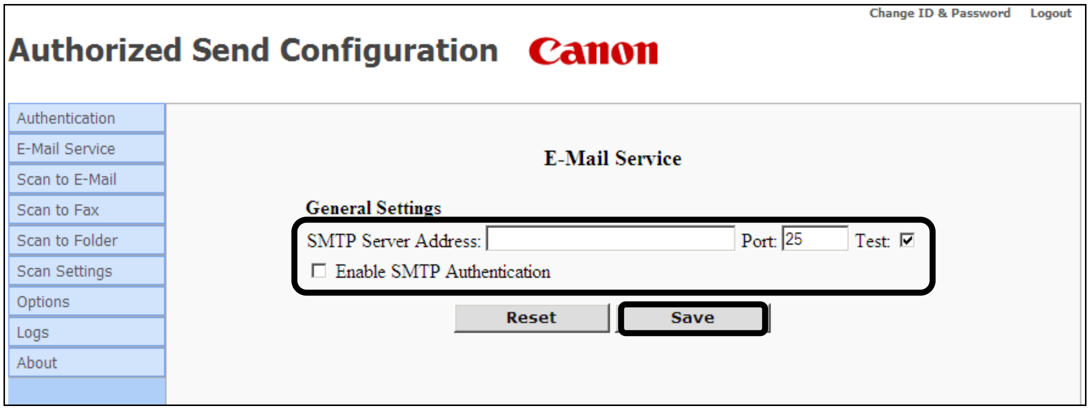


Authentication Servers

	Domain Name	Authentication Method
□	auth.asend.com	Kerberos

   The E-Mail Service screen is displayed.

6. Configure the settings under <General Settings> ➞ click [Save]. (See “Configuring E-Mail Service Settings,” on p. 65.)



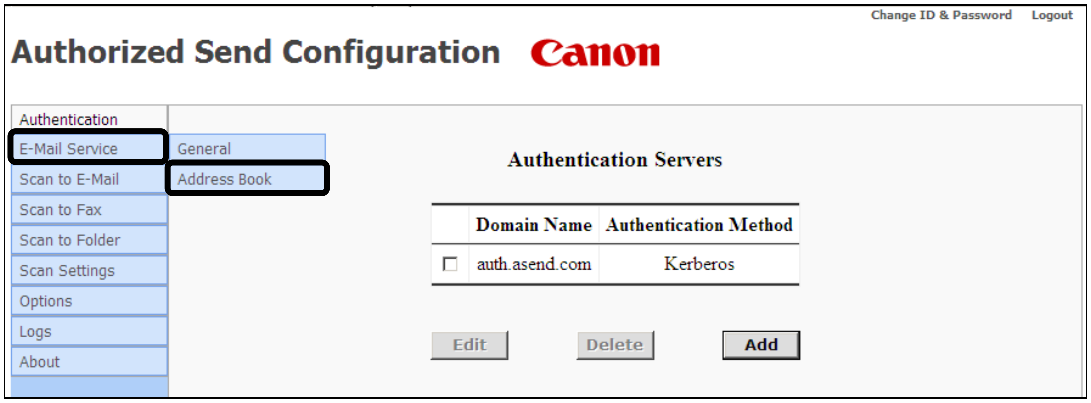
E-Mail Service

General Settings

SMTP Server Address: Port: 25 Test: ☑

☐ Enable SMTP Authentication

7. Click [E-Mail Service] ➞ [Address Book].

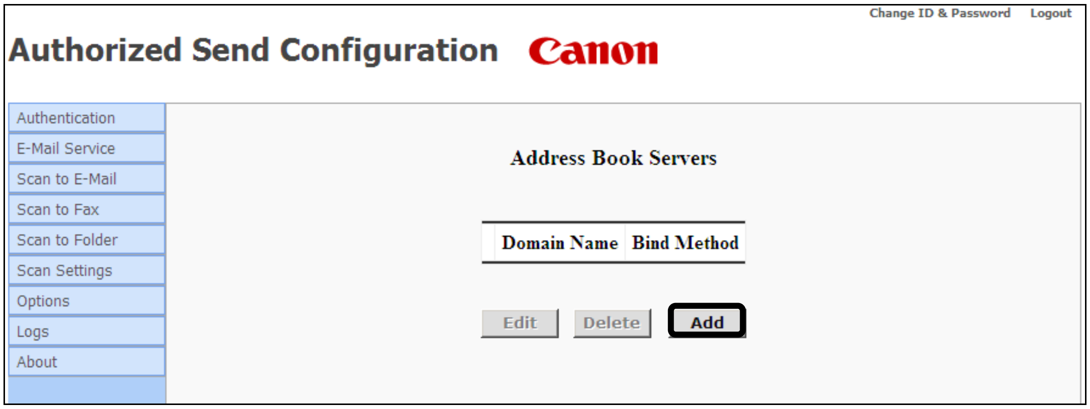


Authentication Servers

	Domain Name	Authentication Method
☐	auth.asend.com	Kerberos

The Address Book Servers screen is displayed.

8. Click [Add].

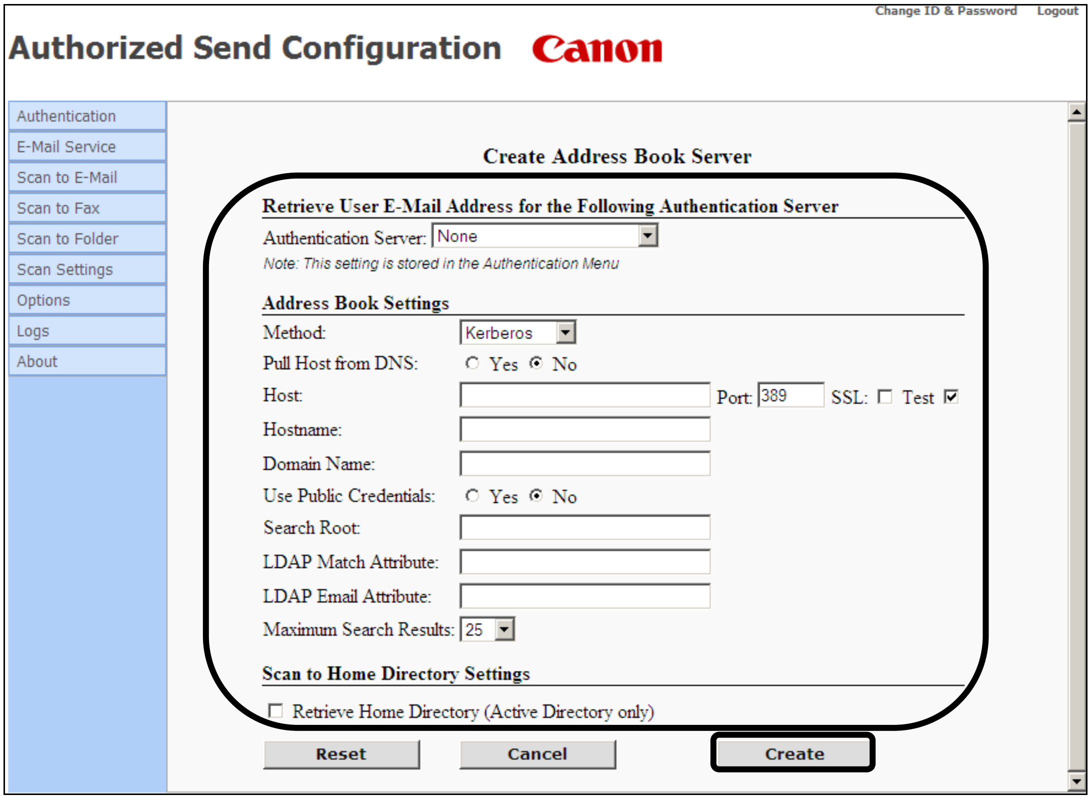


Address Book Servers

Domain Name	Bind Method

The Create Address Book Server screen is displayed.

9. Configure the settings on the Create Address Book Server screen ➞ click [Create].



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: Kerberos

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test ☑

Hostname:

Domain Name:

Use Public Credentials: ○ Yes ● No

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

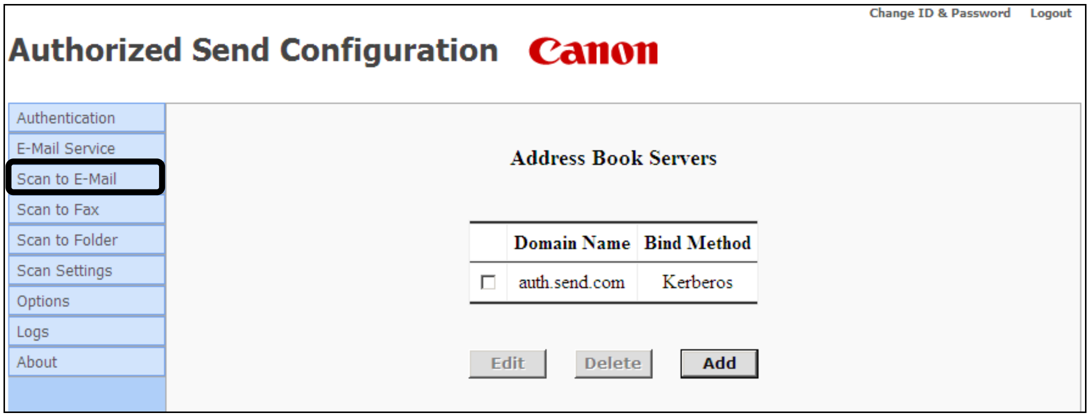
Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

The address book server is created, and is added to the list on the Address Book Servers screen.

10. Click [Scan to E-Mail].

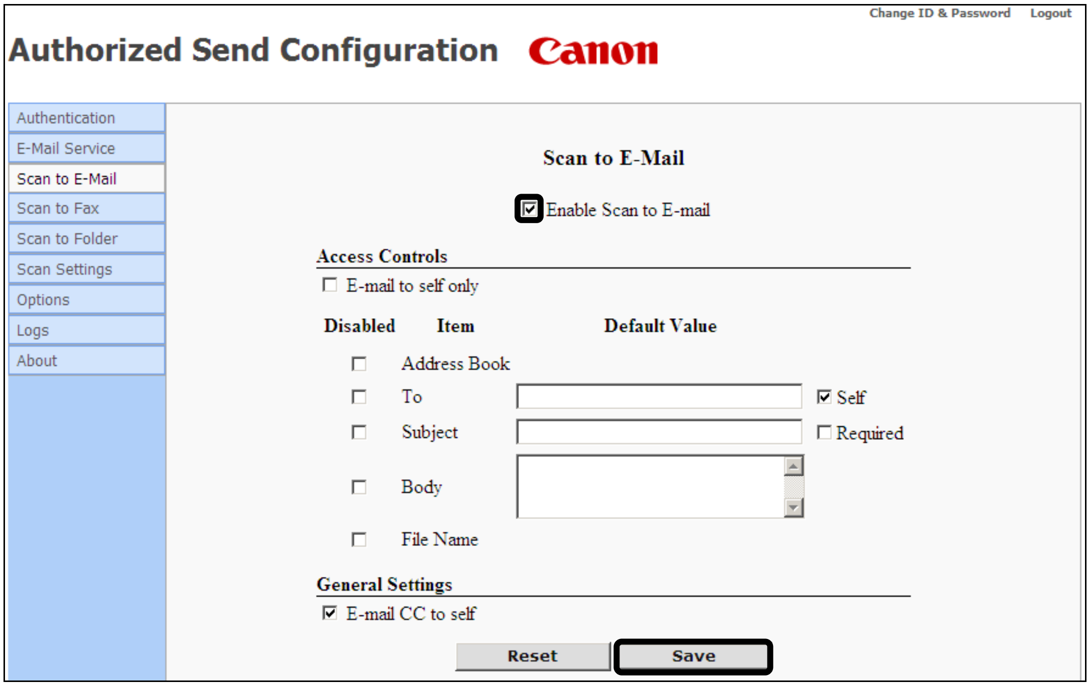


Address Book Servers

	Domain Name	Bind Method
□	auth.send.com	Kerberos

The Scan to E-Mail screen is displayed.

11. Click the [Enable Scan to E-mail] check box ➞ click [Save].



Scan to E-Mail

☑ Enable Scan to E-mail

Access Controls

□ E-mail to self only

Disabled	Item	Default Value	
□	Address Book		
□	To		☑ Self
□	Subject		□ Required
□	Body		
□	File Name		

General Settings

☑ E-mail CC to self

If you want to restrict users to only send e-mail messages to themselves, select the [E-mail to self only] check box.

If you want to restrict access to the [Address Book] key or the [To], [Subject], [Body], or [File Name] text boxes on the SCAN TO EMAIL screen on the machine, select the respective check boxes under <Disabled>.

If you want to restrict the [To] text box to only show the user’s e-mail address, select the [Self] check box.

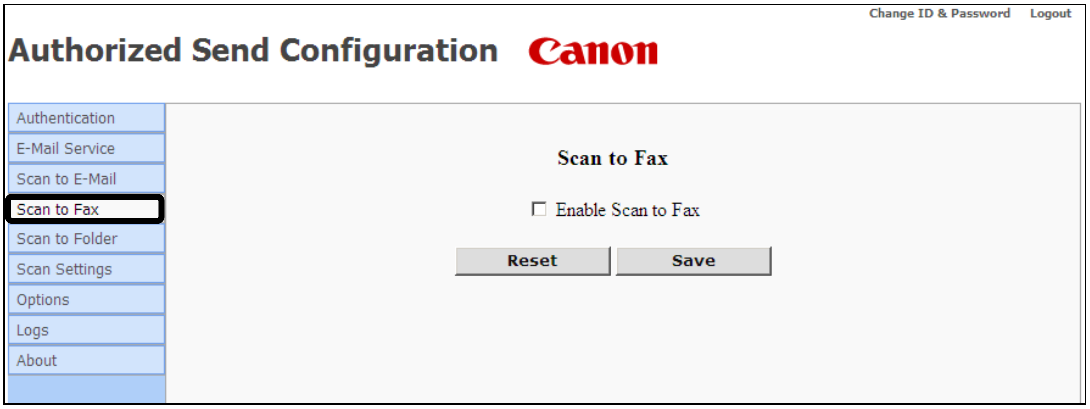
If you require that the [Subject] text box is always populated, select the [Required] check box.

You can set up default recipients, subjects, and body text by entering their default values in the [To], [Subject], and [Body] text boxes under <Default Value>.

If you want to send a copy of the scanned document to the e-mail address registered to your user account, select the [E-mail CC to self] check box.

A message is displayed, informing you that the settings have been saved.

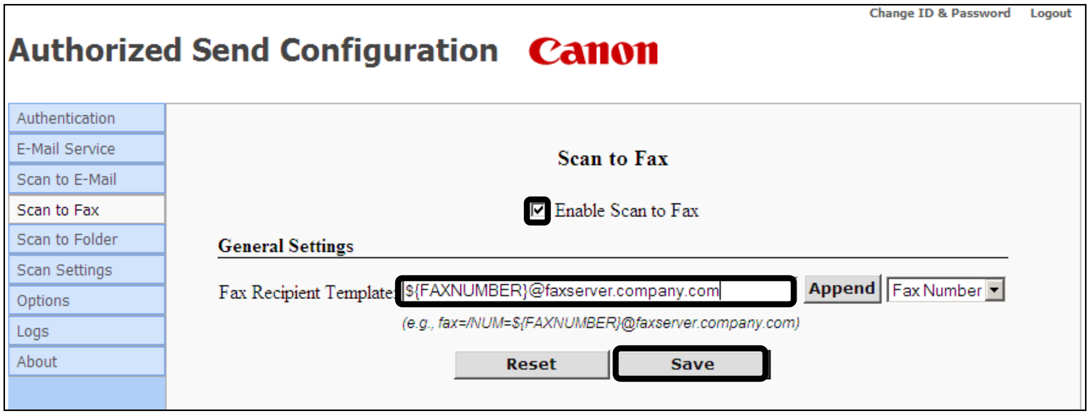
12. Click [Scan to Fax].



□ Enable Scan to Fax

The Scan to Fax screen is displayed.

13. Click the [Enable Scan to Fax] check box ➞ enter the appropriate template configuration in the [Fax Recipient Template] text box ➞ click [Save]. (See "Configuring Scan to Fax Settings," on p. 97.)



☑ Enable Scan to Fax

Fax Recipient Template: ${FAXNUMBER}@faxserver.company.com

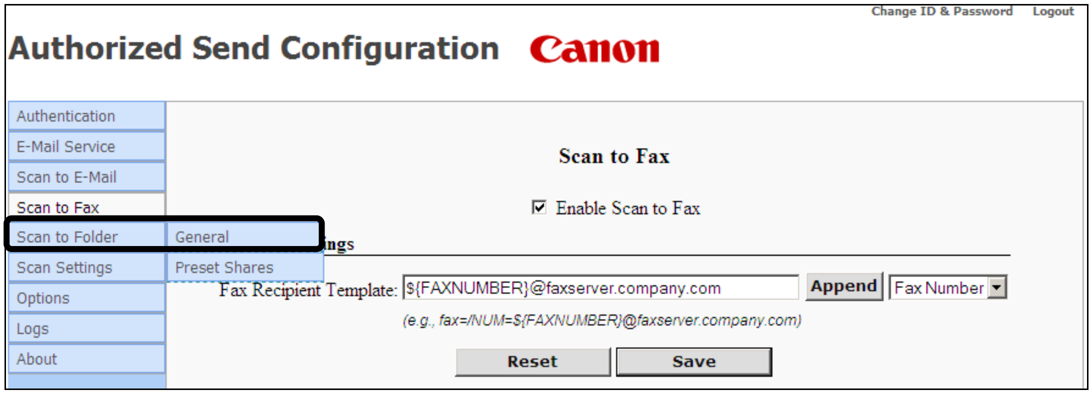
(e.g., fax=/NUM=${FAXNUMBER}@faxserver.company.com)

A message is displayed, informing you that the settings have been saved.

NOTE

The Scan to Fax function is disabled by default.

14. Click [Scan to Folder] ➞ [General].



Scan to Fax

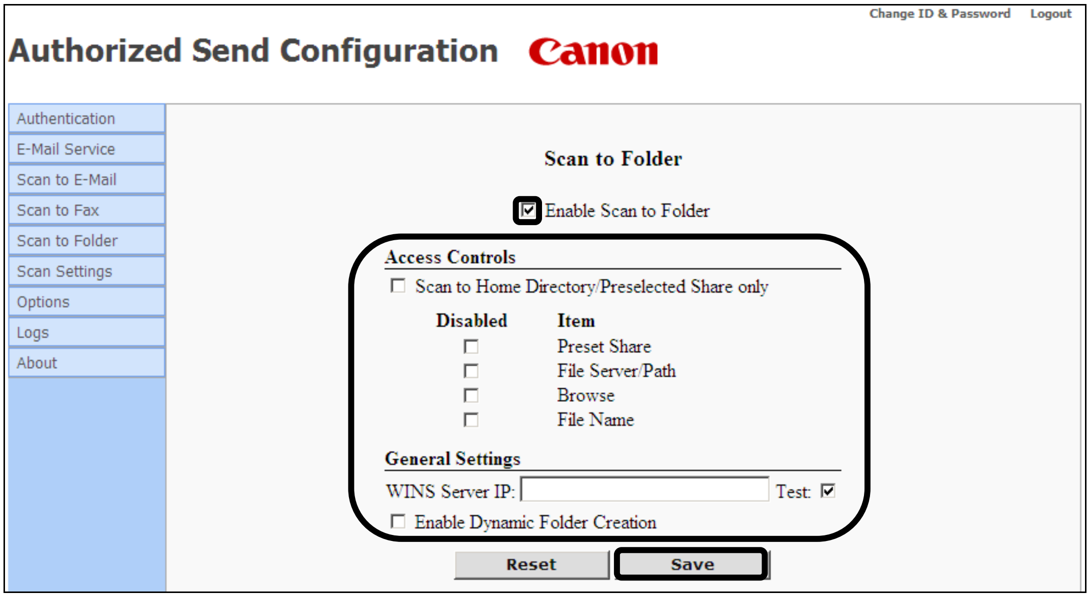
☑ Enable Scan to Fax

Fax Recipient Template: ${FAXNUMBER}@faxserver.company.com

(e.g., fax=/NUM=${FAXNUMBER}@faxserver.company.com)

The Scan to Folder screen is displayed.

15. Select the [Enable Scan to Folder] check box ➞ configure the Scan to Folder Access Controls ➞ enter the IP address of the NetBIOS name server in [WINS Server IP] ➞ click [Save].



Scan to Folder

☑ Enable Scan to Folder

Access Controls

☐ Scan to Home Directory/Preselected Share only

Disabled	Item
☐	Preset Share
☐	File Server/Path
☐	Browse
☐	File Name

General Settings

WINS Server IP: Test: ☑

☐ Enable Dynamic Folder Creation

Select the [Scan to Home Directory/Preselected Share only] check box if you want to automatically disable the [Preset Share], [File Server/Path], and [Browse] check boxes with one click.

If you want to manually restrict user access to the Preset Share drop-down list, File Server and File Path text boxes, Browse key, or File Name text box on the SCAN TO FOLDER screen on the machine, select the [Preset Share], [File Server/Path], [Browse], or [File Name] check boxes under <Disabled>.

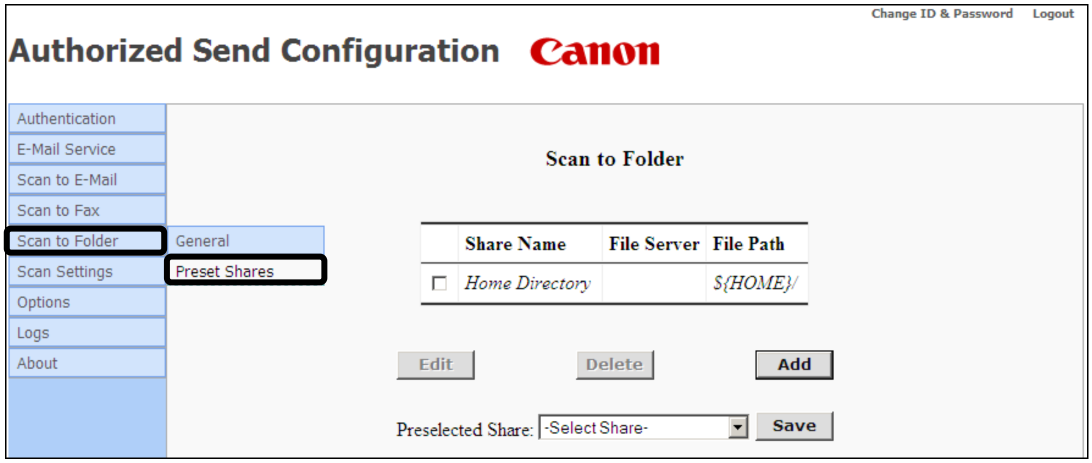
Select the [Test] check box if you want the connection to the WINS server to be verified before you save the settings.

Select the [Enable Dynamic Folder Creation] check box if you want a sub-folder to be automatically created when a user tries to scan to a folder that does not exist.

Select the [Only for Preset Shares] check box to restrict a user to only scan to a dynamic folder that was created as a preset share by the System Administrator beforehand. When this option is selected, the user must enter a valid file server/file path manually.

A message is displayed, informing you that the settings have been saved.

16. Click [Scan to Folder] ➞ [Preset Shares].



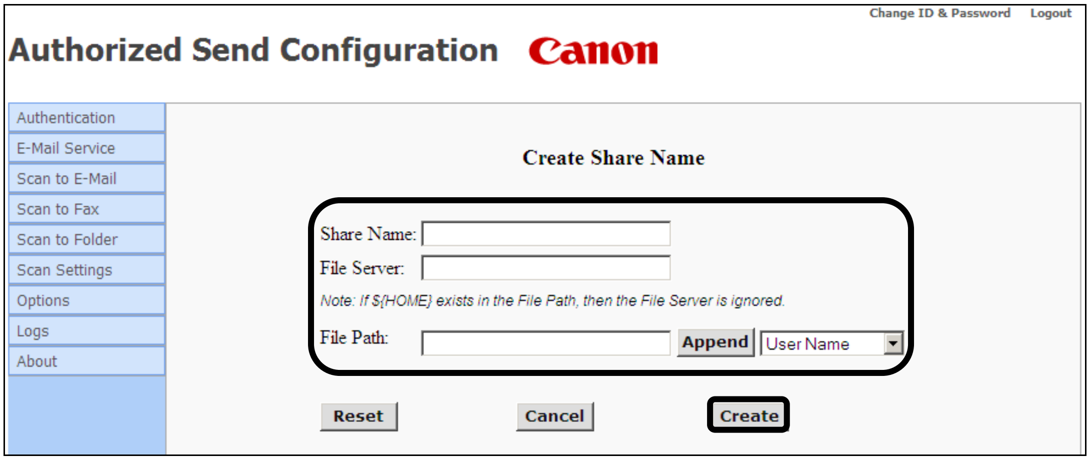
Scan to Folder

	Share Name	File Server	File Path
□	*Home Directory*		*${HOME}/*

Preselected Share: -Select Share- ▾

The Preset Shares screen is displayed.

17. Click [Add] ➞ specify the Share Name settings ➞ click [Create]. (See "Creating a Preset Share," on p. 103.)



Authorized Send Configuration

Create Share Name

Share Name:

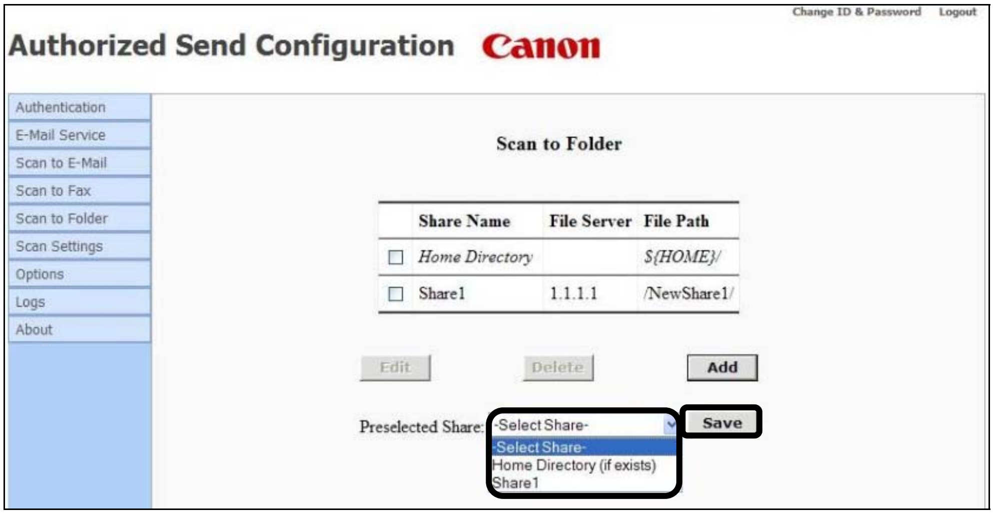
File Server:

Note: If ${HOME} exists in the File Path, then the File Server is ignored.

File Path: Append User Name

The new preset share is added to the list on the Preset Shares screen.

17.1 If you want to specify your home directory as a preselected share that will automatically appear in the Preset Share drop-down list on the SCAN TO FOLDER screen, select [Home Directory (if exists)] from the Preselected Share drop-down list ➞ click [Save]. (See "Creating a Preset Share," on p. 103.)



Authorized Send Configuration

Scan to Folder

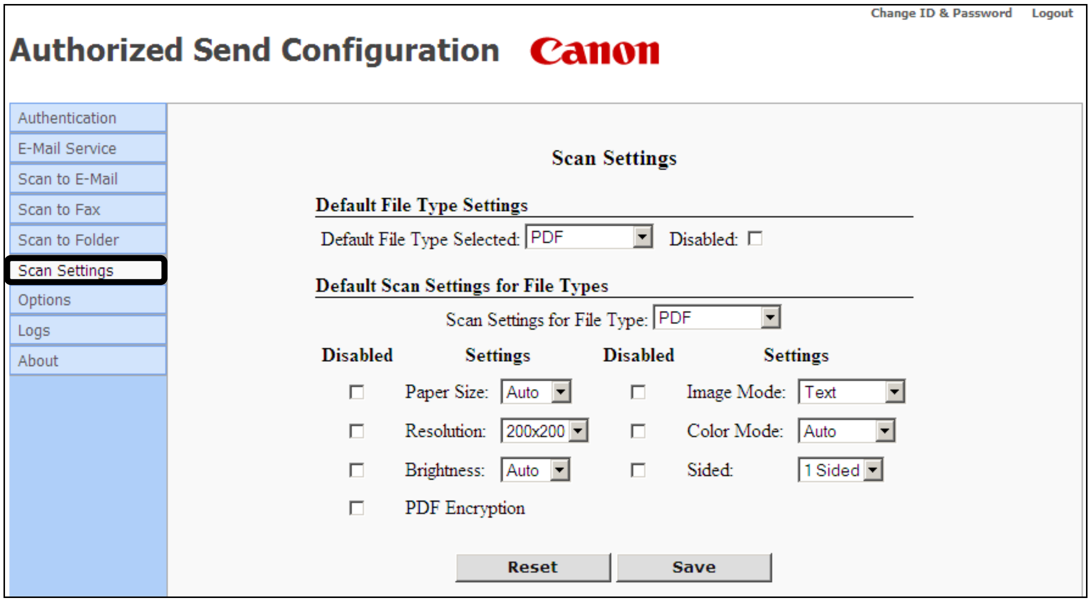
	Share Name	File Server	File Path
□	*Home Directory*		*${HOME}/*
□	Share1	1.1.1.1	/NewShare1/

Preselected Share: -Select Share-

-Select Share-
Home Directory (if exists)
Share1

A message is displayed, informing you that the settings have been saved.

18. Click [Scan Settings]



Scan Settings

Default File Type Settings

Default File Type Selected: PDF Disabled: □

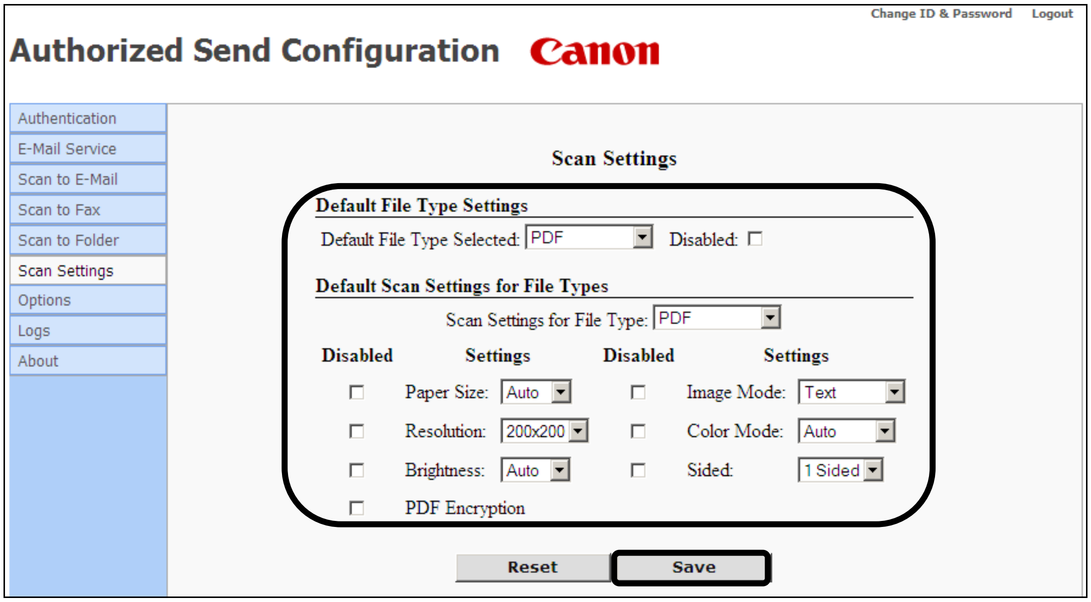
Default Scan Settings for File Types

Scan Settings for File Type: PDF

Disabled	Settings		Disabled	Settings	
□	Paper Size:	Auto	□	Image Mode:	Text
□	Resolution:	200x200	□	Color Mode:	Auto
□	Brightness:	Auto	□	Sided:	1 Sided
□	PDF Encryption				

The Scan Settings screen is displayed.

19. Specify the scan settings, as necessary ➞ click [Save]. (See "Configuring Scan Settings," on p. 108.)



Scan Settings

Default File Type Settings

Default File Type Selected: PDF Disabled: □

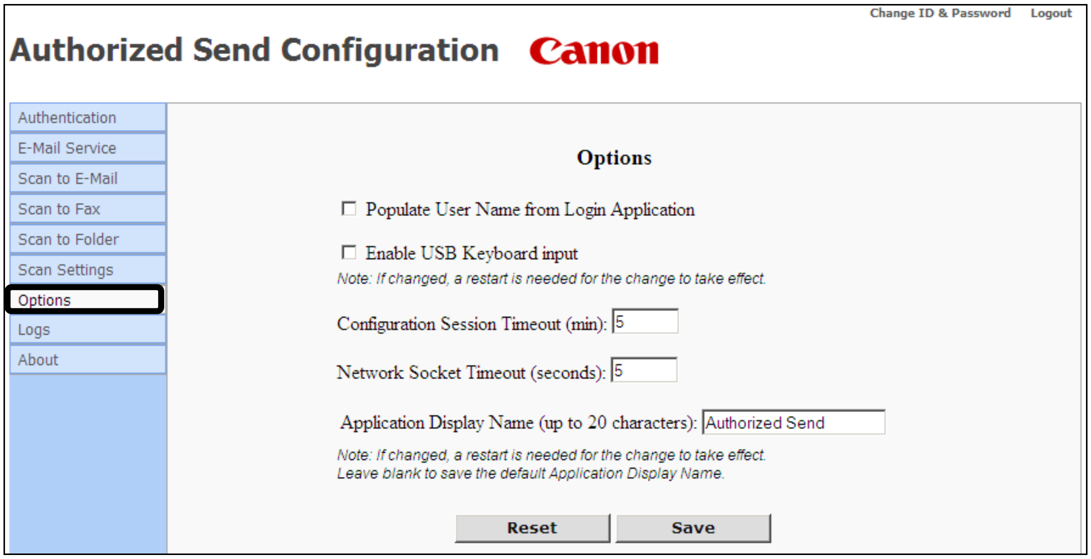
Default Scan Settings for File Types

Scan Settings for File Type: PDF

Disabled	Settings		Disabled	Settings	
□	Paper Size:	Auto	□	Image Mode:	Text
□	Resolution:	200x200	□	Color Mode:	Auto
□	Brightness:	Auto	□	Sided:	1 Sided
□	PDF Encryption				

A message is displayed, informing you that the settings have been saved.

20. Click [Options].



Authorized Send Configuration

Options

☐ Populate User Name from Login Application

☐ Enable USB Keyboard input

Note: If changed, a restart is needed for the change to take effect.

Configuration Session Timeout (min): 5

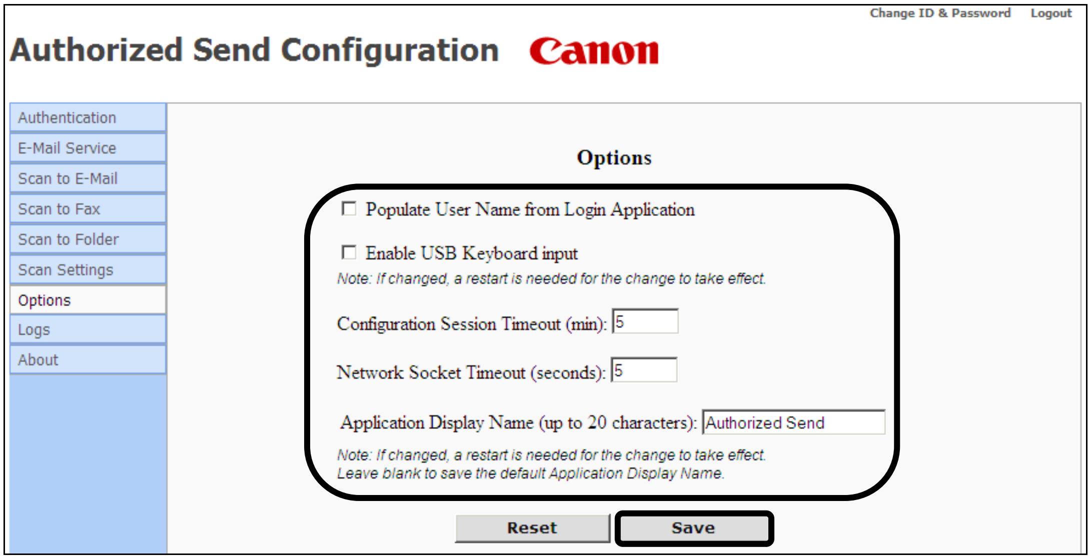
Network Socket Timeout (seconds): 5

Application Display Name (up to 20 characters): Authorized Send

Note: If changed, a restart is needed for the change to take effect.
Leave blank to save the default Application Display Name.

The Options screen is displayed.

21. Specify the optional settings, as necessary ➞ click [Save]. (See “Configuring Optional Settings,” on p.113.)



Authorized Send Configuration

Options

☐ Populate User Name from Login Application

☐ Enable USB Keyboard input

Note: If changed, a restart is needed for the change to take effect.

Configuration Session Timeout (min): 5

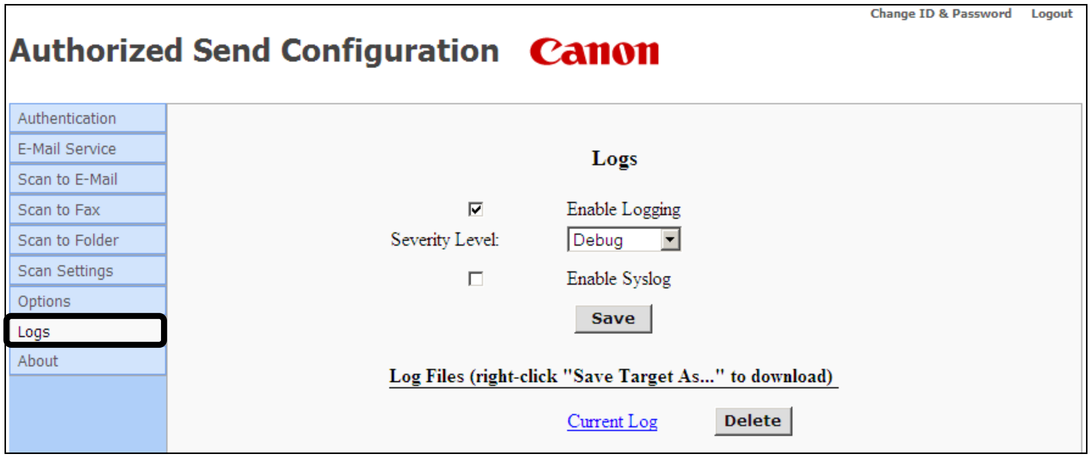
Network Socket Timeout (seconds): 5

Application Display Name (up to 20 characters): Authorized Send

Note: If changed, a restart is needed for the change to take effect.
Leave blank to save the default Application Display Name.

A message is displayed, informing you that the settings have been saved.

22. Click [Logs].



Authorized Send Configuration

Logs

☑ Enable Logging

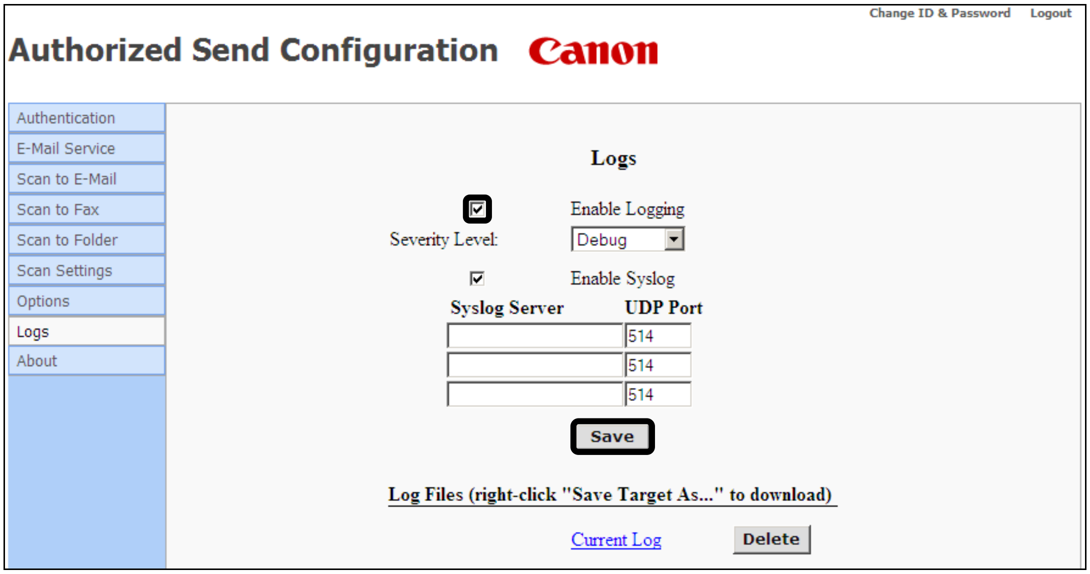
Severity Level: Debug

□ Enable Syslog

Log Files (right-click "Save Target As..." to download)

The Logs screen is displayed.

23. Check the [Enable Logging] check box ➞ specify the Severity Level ➞ configure the syslog servers ➞ click [Save]. (See "Configuring Log Settings," on p. 117.)



Authorized Send Configuration

Logs

☑ Enable Logging

Severity Level: Debug

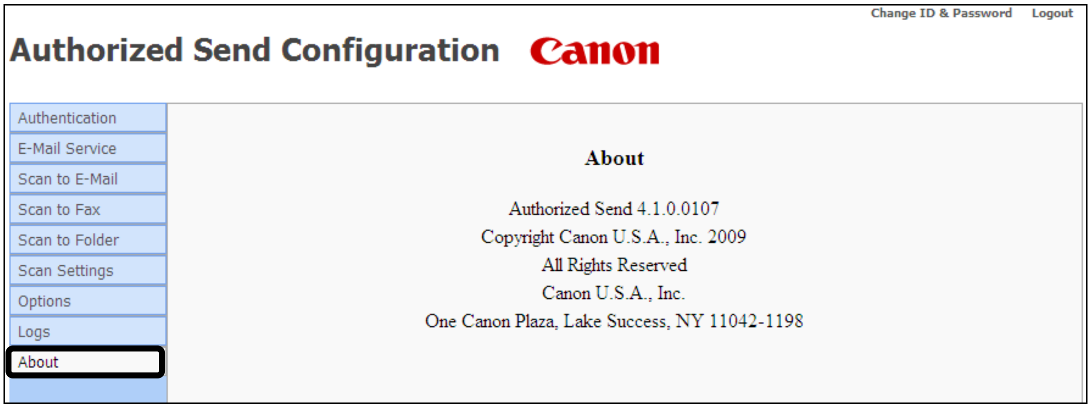
☑ Enable Syslog

Syslog Server	UDP Port
	514
	514
	514

Log Files (right-click "Save Target As..." to download)

You can also view, download, or delete the current log file. For more information, see "Configuring Log Settings," on p. 117.

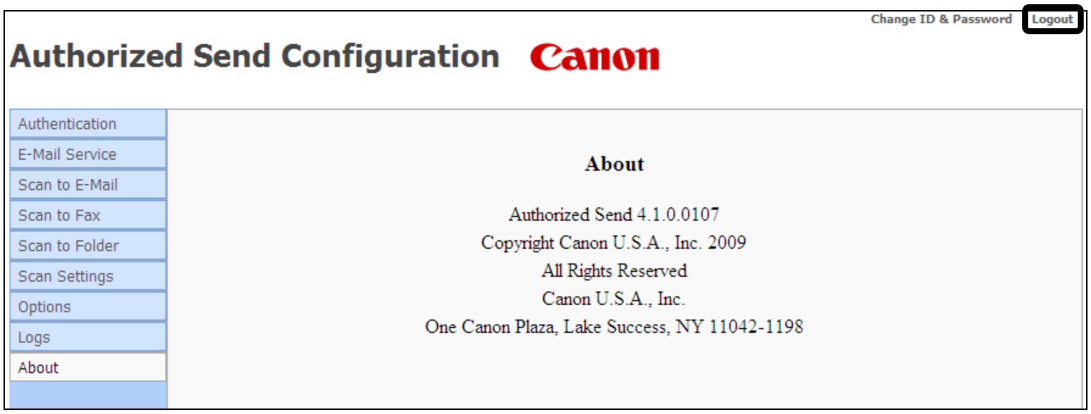
24. If you want to verify the version number of Authorized Send, click [About].



About

Authorized Send 4.1.0.0107
Copyright Canon U.S.A., Inc. 2009
All Rights Reserved
Canon U.S.A., Inc.
One Canon Plaza, Lake Success, NY 11042-1198

25. Click [Logout].



About

Authorized Send 4.1.0.0107
Copyright Canon U.S.A., Inc. 2009
All Rights Reserved
Canon U.S.A., Inc.
One Canon Plaza, Lake Success, NY 11042-1198

3.2 Creating an Authentication Server

You can create up to 10 domains for authentication.

IMPORTANT

If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 142.

1. Display the Authorized Send Configuration screen.

NOTE

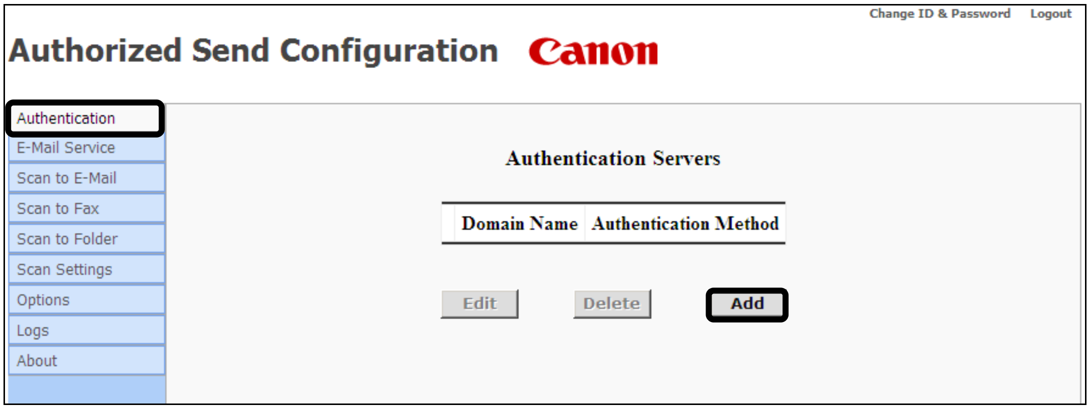
For instructions on displaying the Authorized Send Configuration screen, see "Flow of Configuration Operations," on p. 35.

2. Enter your user name in [Login ID] and your password in [Password] ➞ click [Login].

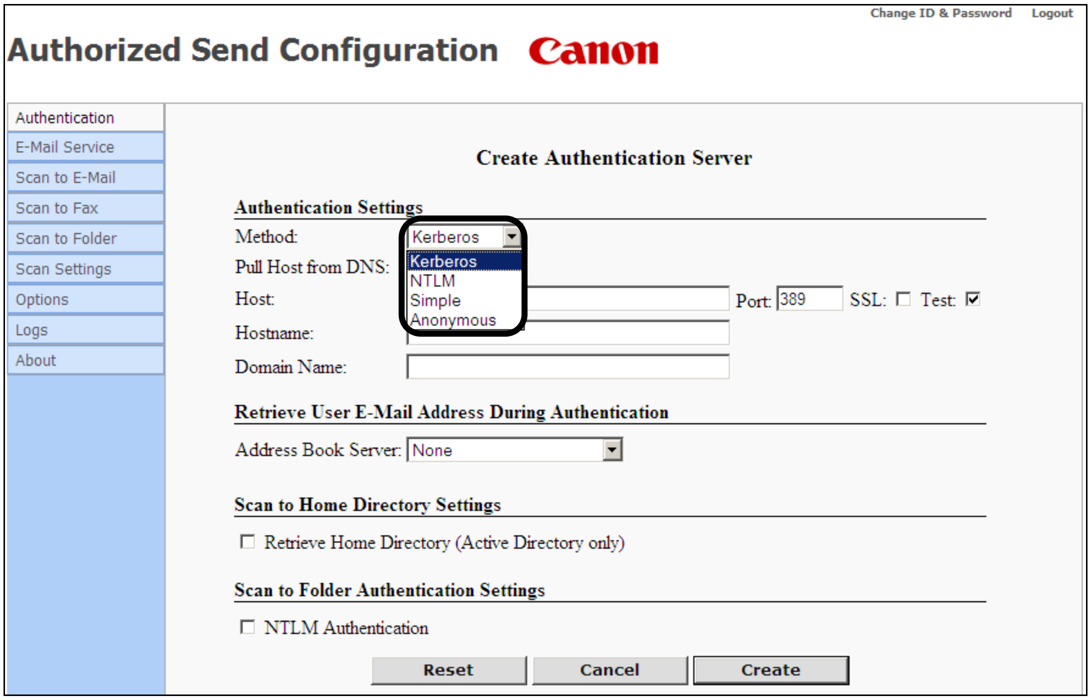
NOTE

For more details on logging on to the Authorized Send Configuration screen, see "Flow of Configuration Operations," on p. 35.

3. Click [Authentication] ➞ [Add].



4. Click the Method drop-down list to select the authentication method.



Create Authentication Server

Authentication Settings

Method: Kerberos

Pull Host from DNS:

Host: Port: 389 SSL: □ Test: ☑

Hostname:

Domain Name:

Retrieve User E-Mail Address During Authentication

Address Book Server: None

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Scan to Folder Authentication Settings

□ NTLM Authentication

[Kerberos]: The machine communicates directly to Active Directory.

[NTLM]: The machine communicates directly to Active Directory.

[Simple]: Necessary if you use Domino or eDirectory for authentication.

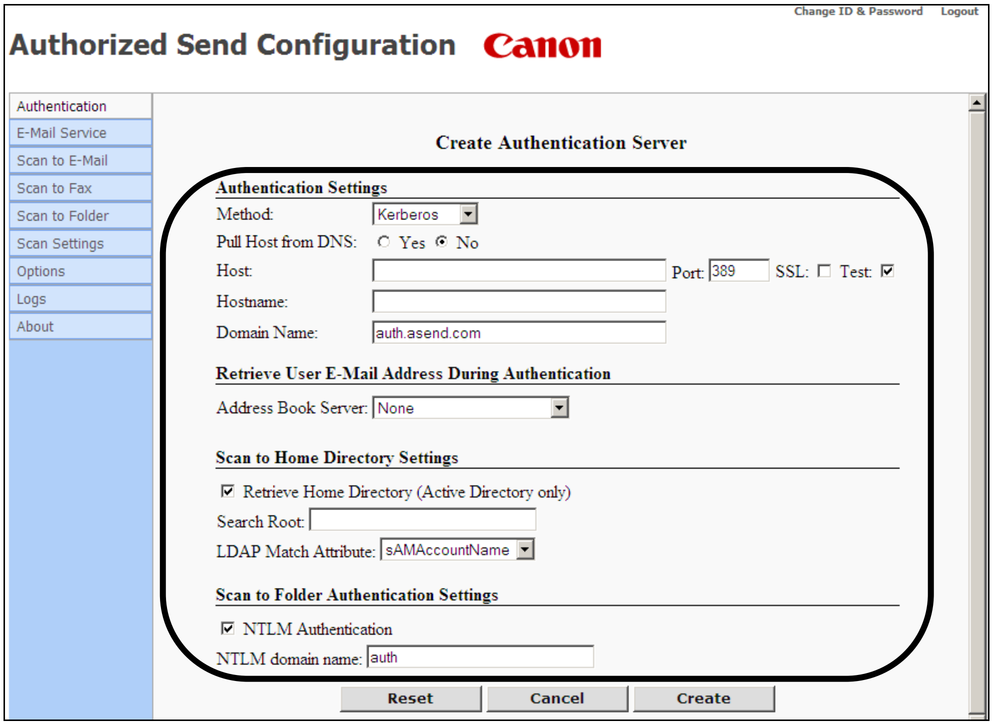
[Anonymous]: Configuring an anonymous authentication server enables you to use Authorized Send without logging on to the application.

IMPORTANT

- If an Anonymous authentication server is configured, the Authorized Send SIGN IN screen on the machine is always bypassed, and the user is logged in as an anonymous user.
- If an Anonymous server is created, other servers cannot be used.
- To disable Anonymous authentication, the Anonymous authentication server must be deleted. When Anonymous authentication is deleted, the default screen is the Authorized Send SIGN IN screen on the machine. For details about deleting an Anonymous authentication server, see "Deleting an Authentication Server," on p. 64.

5. Specify the settings for the selected authentication method.

5.1 If you select [Kerberos] as the authentication method, specify the Authentication Settings, Retrieve User E-Mail Address During Authentication, Scan to Home Directory Settings, and Scan to Folder Authentication Settings.



Authorized Send Configuration

Create Authentication Server

Authentication Settings

Method: Kerberos

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test: ☑

Hostname:

Domain Name: auth.asend.com

Retrieve User E-Mail Address During Authentication

Address Book Server: None

Scan to Home Directory Settings

☑ Retrieve Home Directory (Active Directory only)

Search Root:

LDAP Match Attribute: sAMAccountName

Scan to Folder Authentication Settings

☑ NTLM Authentication

NTLM domain name: auth

Authentication Settings

Method: Kerberos

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is ‘No’.

If you select the [Yes] radio button, the first “live” domain controller is used as the authentication server after you click [Create].

Host: This text box is only displayed if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the authentication server.

Port: This text box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: This check box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: This check box is only displayed if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Hostname: This text box is only displayed for Kerberos if Pull Host from DNS is set to ‘No’. Enter the host name of the authentication server.

Domain Name: Enter the domain name of the authentication server.

Pull Port from DNS: This check box is only displayed if Pull Host from DNS is set to ‘Yes’. Select the [Pull Port from DNS] check box if you want the Port text box to be dynamically populated from the DNS.

Retrieve User E-Mail Address During Authentication

Address Book Server: If you have already configured an address book server select the address book server from which your e-mail address will be retrieved from the drop-down list.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user’s home directory information from the authentication server. This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only)] check box on the Create Address Book Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

Search Root: Specify the search root for searching the user’s home directory via LDAP.

Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.

[Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected.

LDAP Match Attribute: Select [sAMAccountName] or [userPrincipalName] from the drop-down list. This enables you to search for the user’s Home Directory.

Scan to Folder Authentication Settings

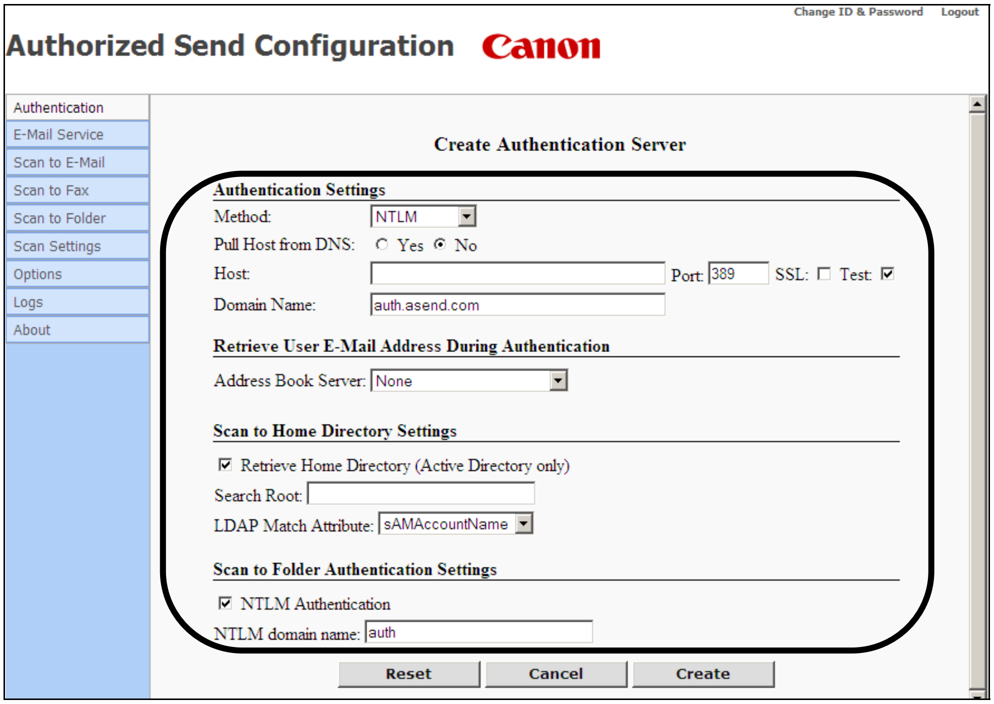
NTLM Authentication: Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.

NTLM domain name: Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature.

IMPORTANT

If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see "Synchronizing the Device and Server Time," on p. 142.

5.2 If you select [NTLM] as the authentication method, specify the Authentication Settings, Retrieve User E-Mail Address During Authentication, Scan to Home Directory Settings, and Scan to Folder Authentication Settings.



Create Authentication Server

Authentication Settings

Method: NTLM

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test: ☑

Domain Name: auth.asend.com

Retrieve User E-Mail Address During Authentication

Address Book Server: None

Scan to Home Directory Settings

☑ Retrieve Home Directory (Active Directory only)

Search Root:

LDAP Match Attribute: sAMAccountName

Scan to Folder Authentication Settings

☑ NTLM Authentication

NTLM domain name: auth

Authentication Settings

Method: NTLM

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is ‘No’.

If you select the [Yes] radio button, the first “live” domain controller is used as the authentication server after you click [Create].

Host: This text box is only displayed if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the authentication server.

Port: This text box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: This check box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: This check box is only displayed if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name: Enter the domain name of the authentication server.

Pull Port from DNS: This check box is only displayed if Pull Host from DNS is set to ‘Yes’. Select the [Pull Port from DNS] check box if you want the Port text box to be dynamically populated from the DNS.

Retrieve User E-Mail Address During Authentication

Address Book Server: If you have already configured an address book server select the address book server from which your e-mail address will be retrieved from the drop-down list.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user's home directory information from the authentication server. This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only)] check box on the Create Address Book Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

Search Root: Specify the search root for searching the user's home directory via LDAP.

Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.

[Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected.

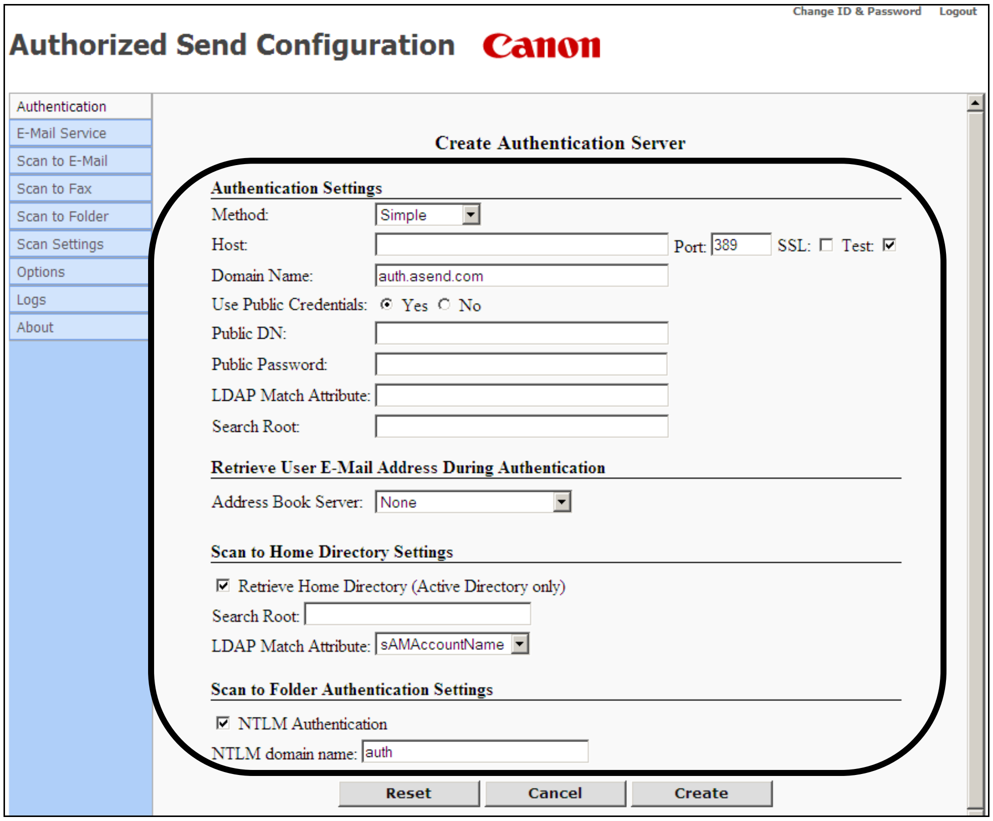
LDAP Match Attribute: Select [sAMAccountName] or [userPrincipalName] from the drop-down list. This enables you to search for the user's Home Directory.

Scan to Folder Authentication Settings

NTLM Authentication: Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.

NTLM domain name: Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature.

5.3 If you select [Simple] as the authentication method, specify the Authentication Settings, Retrieve User E-Mail Address During Authentication, Scan to Home Directory Settings, and Scan to Folder Authentication Settings.



Authorized Send Configuration

Create Authentication Server

Authentication Settings

Method: Simple

Host: Port: 389 SSL: □ Test: ☑

Domain Name: auth.asend.com

Use Public Credentials: ● Yes ○ No

Public DN:

Public Password:

LDAP Match Attribute:

Search Root:

Retrieve User E-Mail Address During Authentication

Address Book Server: None

Scan to Home Directory Settings

☑ Retrieve Home Directory (Active Directory only)

Search Root:

LDAP Match Attribute: sAMAccountName

Scan to Folder Authentication Settings

☑ NTLM Authentication

NTLM domain name: auth

Authentication Settings

Method: Simple

Host: Enter the DNS name or IP address of the authentication server.

Port: Enter the connecting port number of the authentication server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: Select this check box if you want the authentication server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: Select this check box if you want the connection to the authentication server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name: Enter the domain name of the authentication server.

Use Public Credentials: Select [Yes] to configure the public credentials (Public DN and Public Password), or select [No] to use anonymous binding.

Public DN: This text box is only displayed if Use Public Credentials is set to ‘Yes’. Enter the user’s login Distinguished Name to use when performing the first bind of the Simple Binding process.

Public Password: This text box is only displayed if Use Public Credentials is set to ‘Yes’. It is used as the password for authentication against the address book server. It is an optional text box, with no limit on the number of characters that can be used.

LDAP Match Attribute: Enter the user name’s LDAP attribute to be matched with the user name when performing the first bind of the Simple Binding process.

Search Root: Enter the root to search for the authenticating user’s Domain Name.

If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.

Retrieve User E-Mail Address During Authentication

Address Book Server: If you have already configured an address book server, select the address book server from which your e-mail address will be retrieved from the drop-down list.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user’s home directory information from the authentication server. This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

> If this check box is selected, and the [Retrieve Home Directory (Active Directory only)] check box on the Create Address Book Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

Search Root: Specify the search root for searching the user’s home directory via LDAP.

[Search Root] only appears if the [Retrieve Home Directory (Active Directory only)] check box is selected.

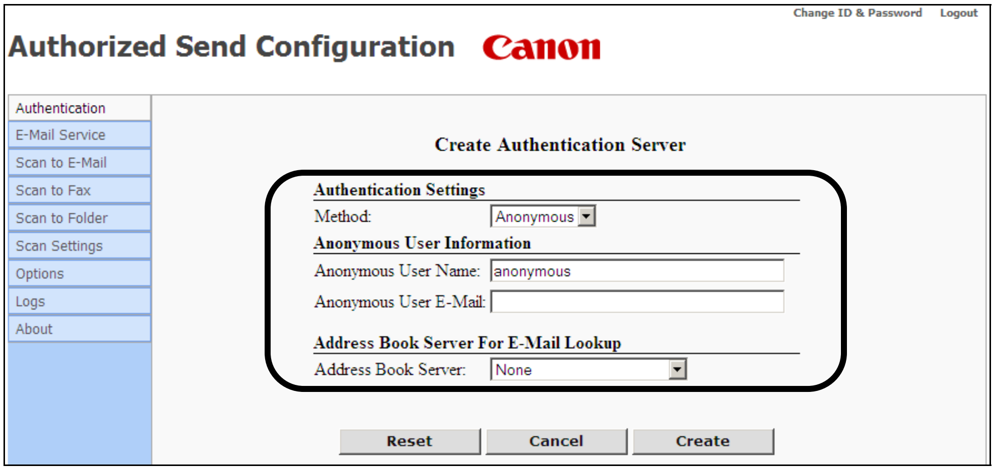
LDAP Match Attribute: Select [sAMAccountName] or [userPrincipalName] from the drop-down list. This enables you to search for the user’s Home Directory.

Scan to Folder Authentication Settings

NTLM Authentication: Select this check box to use NTLM as the authentication method for the Scan to Folder feature, regardless of the authentication method you selected for the authentication server.

NTLM domain name: Enter the domain name to be used for NTLM authentication of a share for the Scan to Folder feature.

5.4 If you select [Anonymous] as the authentication method, specify the Anonymous User Information, and Address Book Server for E-Mail Lookup.



Create Authentication Server

Authentication Settings

Method: Anonymous

Anonymous User Information

Anonymous User Name: anonymous

Anonymous User E-Mail:

Address Book Server For E-Mail Lookup

Address Book Server: None

Authentication Settings

Method: Anonymous

Anonymous User Information

Anonymous User Name: Enter the user name for anonymous sending. You can enter a maximum of 40 characters. Validation cannot occur if this text box is blank. The default setting is ‘anonymous’.

Anonymous User E-Mail: This text box is used as the sender’s e-mail address for the Scan to Fax and Scan to E-Mail functions. Enter the Anonymous user’s e-mail address. You can enter a maximum of 64 characters for the first (local) part, and a maximum of 255 characters for the domain part. This text box is optional.

IMPORTANT

- If an anonymous authentication server is configured, the SIGN IN screen on the machine is bypassed, and the user is logged on as an anonymous user. If more than one Authorized Send function is enabled, the MAIN screen on the machine is displayed. If only one Authorized Send function is enabled, that function's screen is displayed.
- If the [Anonymous User E-Mail] text box is blank, the Scan to Fax and Scan to E-Mail functions do not work on the machine.
- If only one function is enabled but that function is inaccessible due to insufficient data (such as no sender's e-mail address for the SCAN TO EMAIL or SCAN TO FAX screens on the machine), the MAIN screen on the machine is displayed with that function's button disabled and an error message.

NOTE

Validation of the Anonymous User Name and Anonymous User E-Mail occurs when [Create] is clicked. If validation fails, an error message is displayed.

Address Book Server for E-Mail Lookup

Address Book Server:	Select a configured address book server to use with the e-mail lookup feature of the Scan to E-Mail function.

6. Click [Create].

   If you make a mistake while configuring the authentication server settings, click [Reset] to return the settings to their original values.

   To cancel creating the authentication server and return to the Authentication Servers screen, click [Cancel].

   A message is displayed informing you that the configuration has been saved, and the screen returns to the Authentication Servers screen.

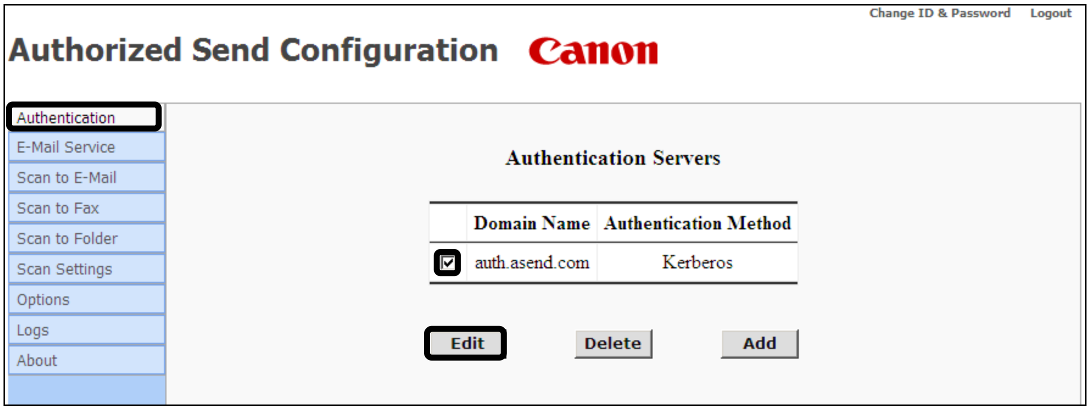
IMPORTANT

- Click the [Test] check box next to <Host> if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message will be displayed. Enter the correct information ➞ click [Save].

3.3 Editing an Authentication Server

You can edit a previously created authentication server from the Authorized Send Configuration screen.

1. Click [Authentication] ➞ select the check box next to the authentication server you want to edit ➞ click [Edit].

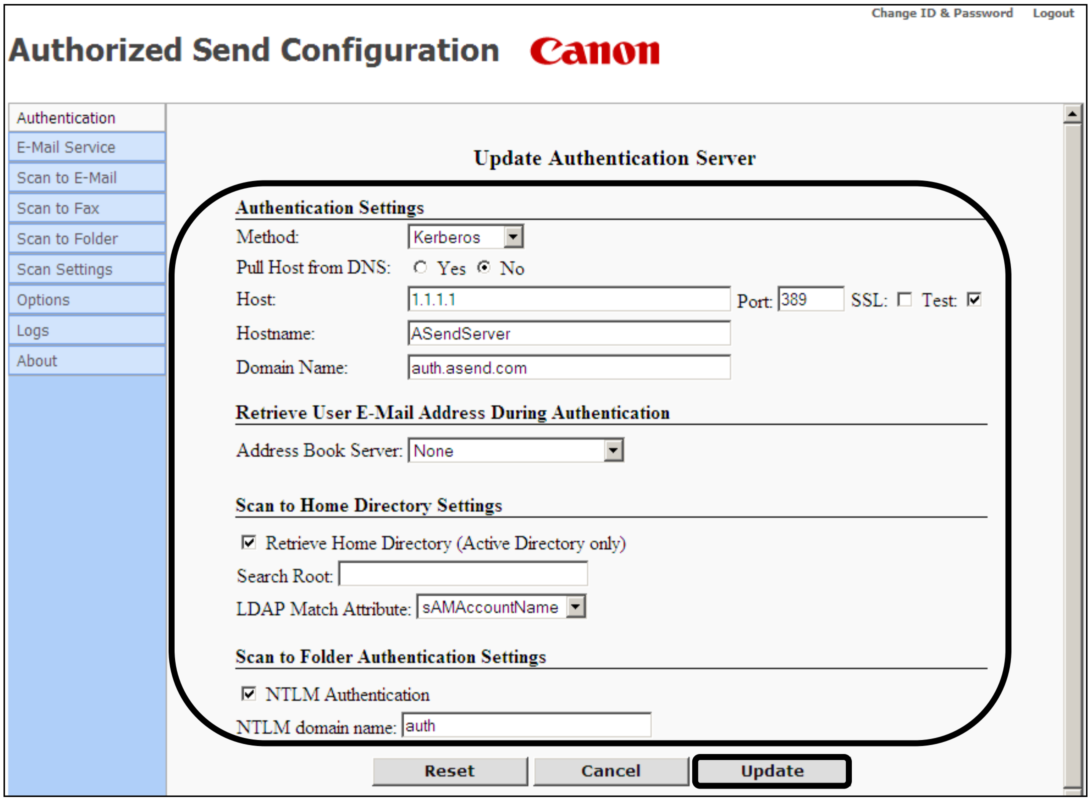


Authorized Send Configuration Canon

Authentication Servers

	Domain Name	Authentication Method
☑	auth.asend.com	Kerberos

2. Edit the settings for the authentication server as necessary ➞ click [Update].



Update Authentication Server

Authentication Settings

Method: Kerberos

Pull Host from DNS: ○ Yes ● No

Host: 1.1.1.1 Port: 389 SSL: □ Test: ☑

Hostname: ASendServer

Domain Name: auth.asend.com

Retrieve User E-Mail Address During Authentication

Address Book Server: None

Scan to Home Directory Settings

☑ Retrieve Home Directory (Active Directory only)

Search Root:

LDAP Match Attribute: sAMAccountName

Scan to Folder Authentication Settings

☑ NTLM Authentication

NTLM domain name: auth

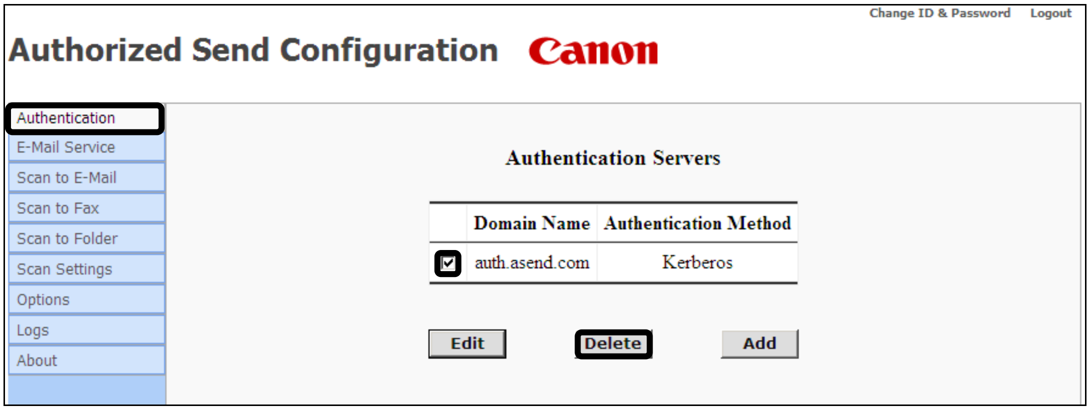
If you make a mistake, click [Reset] to return the settings to their original values.

To cancel editing the authentication server and return to the Authentication Servers screen, click [Cancel].

3.4 Deleting an Authentication Server

You can delete a previously created authentication server from the Authorized Send Configuration screen.

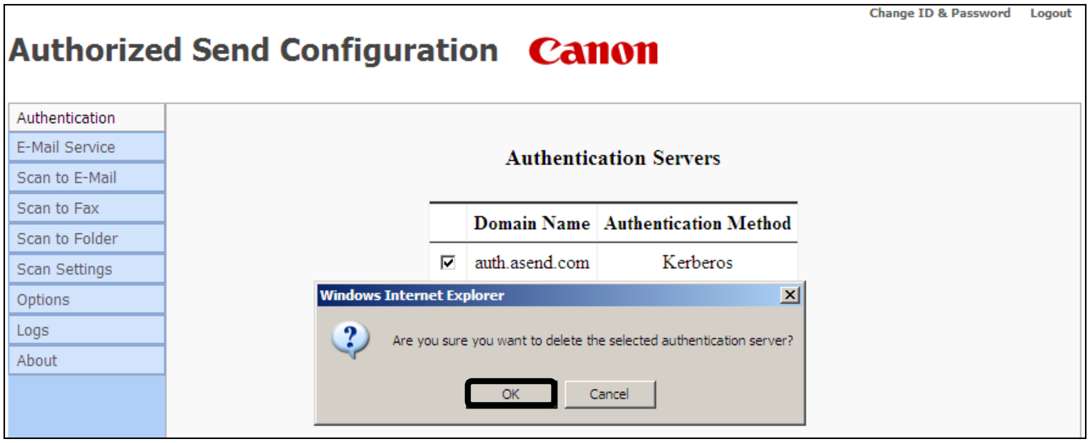
1. Click [Authentication] ➞ select the check box next to the authentication server you want to delete ➞ click [Delete].



Authentication Servers

	Domain Name	Authentication Method
☑	auth.asend.com	Kerberos

2. Click [OK].



Authentication Servers

	Domain Name	Authentication Method
☑	auth.asend.com	Kerberos

Are you sure you want to delete the selected authentication server?

If you do not want to delete the authentication server, click [Cancel].

The authentication server is deleted from the list.

3.5 Configuring the E-Mail Service Settings

You can configure the settings for the SMTP server.

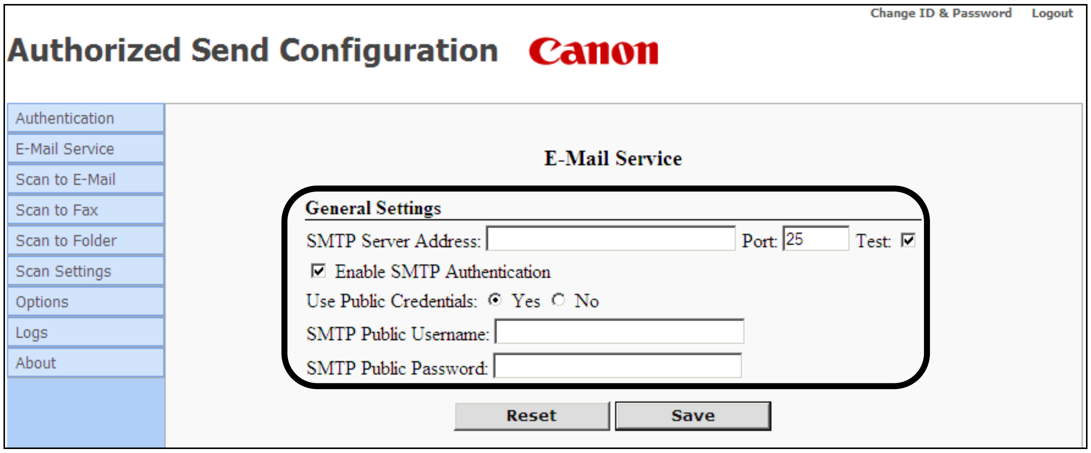
NOTE

The E-Mail Service Settings must be configured to use the Scan to E-Mail and Scan to Fax functions.

1. Click [E-Mail Service] ➞ [General].

   If necessary, see the screen shot in step 5 of "Flow of Configuration Operations," on p. 35.

2. Configure the settings as necessary.



General Settings

SMTP Server Address: Port: 25 Test: ☑

☑ Enable SMTP Authentication

Use Public Credentials: ● Yes ○ No

SMTP Public Username:

SMTP Public Password:

General Settings

SMTP Server Address: Enter the IP Address or DNS name of the SMTP server.

Port: Enter the connecting port number of the SMTP server. You can enter a maximum of five numbers. The default port number is ‘25’.

Test: Select this check box if you want the connection to the SMTP server to be verified before you save the settings. The [Test] check box is selected by default.

Enable SMTP Authentication: Select this check box to have the user authenticated on the SMTP server when using the Scan to E-Mail or Scan to Fax function.

Use Public Credentials: Select [Yes] to configure the SMTP public credentials (Public User Name, Public Password). If [Yes] is selected, enter the user’s SMTP public name and password for SMTP authentication. If [No] is selected, the user’s normal login credentials are used.

SMTP Public Username: If [Yes] is selected for Use Public Credentials, you must enter the user name for SMTP authentication.

SMTP Public Password: If [Yes] is selected for Use Public Credentials, you must enter the password for SMTP authentication.

3. Click [Save].

   If you make a mistake while configuring the settings, click [Reset] to return the settings to their original values.

   A message is displayed informing you that the configuration has been saved.

IMPORTANT

- Click the [Test] check box if you want to test the validity of the IP address you entered before saving.
- If validation fails, an error message will be displayed. Enter the correct information → click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the address you entered, click the check box to clear the check mark.

3.6 Creating an Address Book Server

You can create up to 10 address book Servers.

When you create an address book server, you can either associate it with an authentication server, which has been previously created, or you can create a standalone address book server with no association to an authentication server.

IMPORTANT

- You must configure an address book for an authentication server to retrieve an e-mail address for the end user when authenticating against the authentication server.
- If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see “Synchronizing the Device and Server Time,” on p. 142.

NOTE

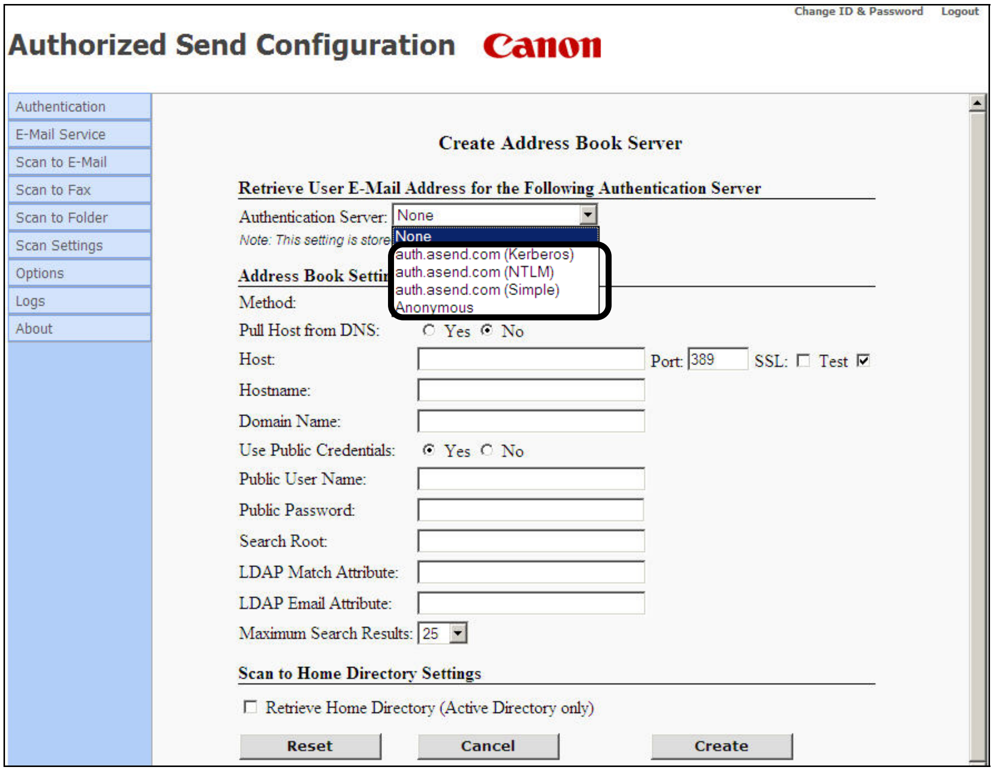
- To associate an address book with an authentication server, you must first create an authentication server for Authorized Send. For instructions on creating an authentication server, see “Creating an Authentication Server,” on p. 49.
- This option may be initially set on this screen, as well as configured and edited on the Create Authentication Server screen.
- If you select [None] from the Authentication Server drop-down list when creating an address book server, the address book server will not be associated with an authentication server and will not interact with any other features of Authorized Send. Select [None] if you want to create an address book server that can be configured at a later time.

1. Click [E-Mail Service] ➞ [Address Book] ➞ [Add] on the Address Book Servers screen.

   If necessary, see the screen shots in steps 7 and 8 of "Flow of Configuration Operations," on p. 35.

2. Specify whether you want to create an address book server with or without an association to an authentication server.

   2.1 If you want to create an address book server with an association to an authentication server, select [Kerberos], [NTLM], [Simple], or [Anonymous] from the Authentication Server drop-down list under <Retrieve User E-Mail Address for the Following Authentication Server>.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is store

None
auth.asend.com (Kerberos)
auth.asend.com (NTLM)
auth.asend.com (Simple)
Anonymous

Address Book Settin

Method:

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test ☑

Hostname:

Domain Name:

Use Public Credentials: ● Yes ○ No

Public User Name:

Public Password:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

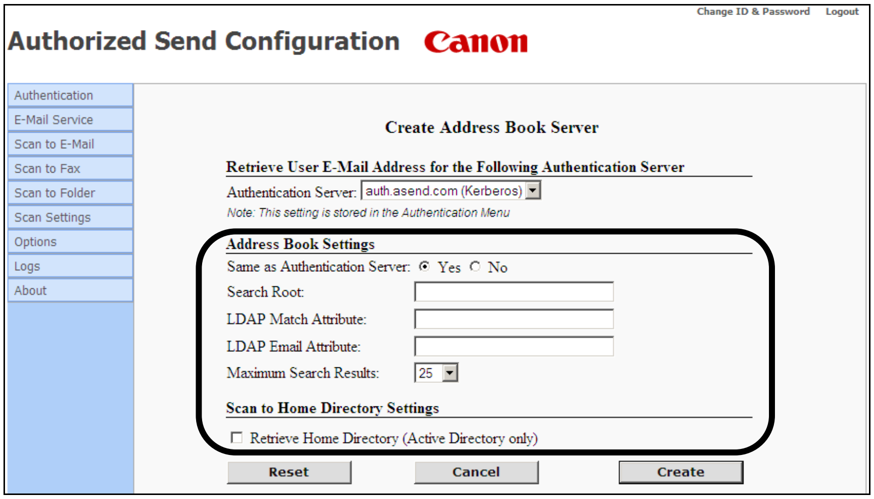
IMPORTANT

If you select [Kerberos], [NTLM], or [Simple] as the authentication server, [Same as Authentication Server] appears as an additional setting under <Address Book Settings>. Select [Yes] to create the address book with the same credentials as the selected authentication server. If you select [No], you must enter the configuration information for the authentication method.

NOTE

The items in the Authentication Server drop-down list correspond to previously registered authentication servers.

2.1.1 If you select a Kerberos or NTLM authentications server, specify the Address Book Settings and Scan to Home Directory Settings ➞ proceed to step 4.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: auth.asend.com (Kerberos)

Note: This setting is stored in the Authentication Menu

Address Book Settings

Same as Authentication Server: ● Yes ○ No

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Address Book Settings

Same as Authentication Server: Select [Yes] to create the address book with the same credentials as the selected authentication server. If you select [No], proceed to step 3 and enter the configuration information for the authentication method.

NOTE

Although step 3 shows a standalone address book server with no association to an authentication server, the configuration information is identical to if you were creating an address book server with an association to an authentication server (except for selecting [None] for the authentication server and not displaying [Same as Authentication Server]).

Search Root: Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.

LDAP Match Attribute: Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Retrieve Home Directory (Active Directory only] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.

An example for Active Directory is ‘sAMAccountName’ or ‘userPrincipalName’.

LDAP Email Attribute: Enter the e-mail LDAP attribute to pull the user’s e-mail address.

An example for Active Directory is ‘mail’.

Maximum Search Results: Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the ADDRESS BOOK screen of the machine. The default setting is ‘25’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user’s home directory information from the address book server with the LDAP attribute of “Home Directory.” This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

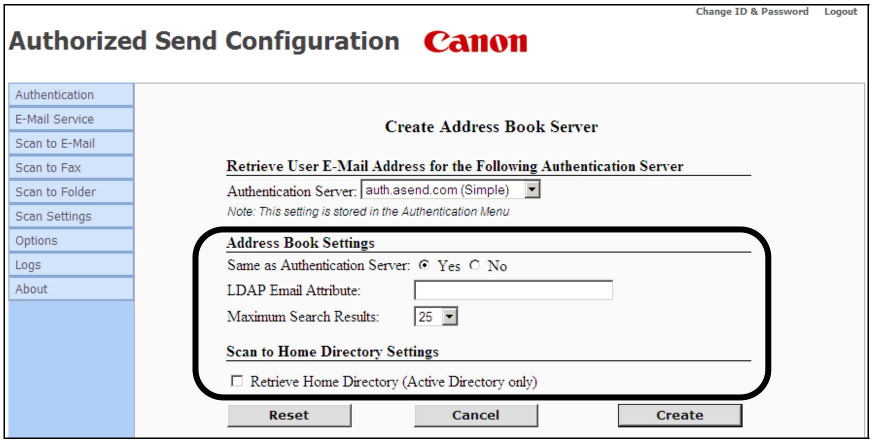
IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

IMPORTANT

If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see “Synchronizing the Device and Server Time,” on p. 142.

2.1.2 If you select a Simple authentication server, specify the Address Book Settings and Scan to Home Directory Settings ➞ proceed to step 4.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: auth.asend.com (Simple)

Note: This setting is stored in the Authentication Menu

Address Book Settings

Same as Authentication Server: ● Yes ○ No

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Address Book Settings

Same as Authentication Server: Select [Yes] to create the address book with the same credentials as the selected authentication server. If you select [No], proceed to step 3 and enter the configuration information for the authentication method.

NOTE

Although step 3 shows a standalone address book server with no association to an authentication server, the configuration information is identical to if you were creating an address book server with an association to an authentication server (except for selecting [None] for the authentication server and not displaying [Same as Authentication Server]).

LDAP Email Attribute: Enter the e-mail LDAP attribute to pull the user’s e-mail address.

An example for Active Directory is ‘mail’.

Maximum Search Results: Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the ADDRESS BOOK screen of the machine. The default setting is ‘25’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only):	Select this check box to obtain the currently logged on user’s home directory information from the address book server with the LDAP attribute of “Home Directory.” This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

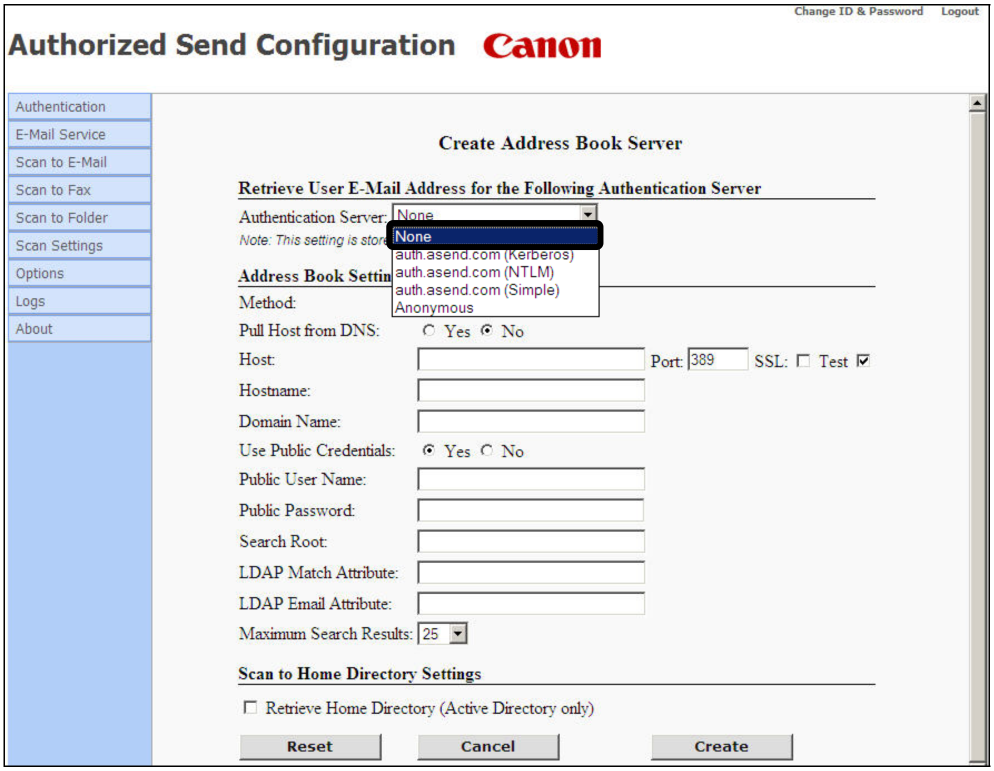
If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

2.1.3 If you select an Anonymous authentication server, proceed to step 3 and enter the configuration information for the authentication method.

NOTE

Although step 3 shows a standalone address book server with no association to an authentication server, the configuration information is identical to if you were creating an address book server with an association to an authentication server (except for selecting [None] for the authentication server and not displaying [Same as Authentication Server]).

2.2 If you want to create a standalone address book server with no association to an authentication server, select [None] from the Authentication Server drop-down list under <Retrieve User E-Mail Address for the Following Authentication Server>.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

None
auth.asend.com (Kerberos)
auth.asend.com (NTLM)
auth.asend.com (Simple)
Anonymous

Note: This setting is stor

Address Book Settin

Method:

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test ☑

Hostname:

Domain Name:

Use Public Credentials: ● Yes ○ No

Public User Name:

Public Password:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

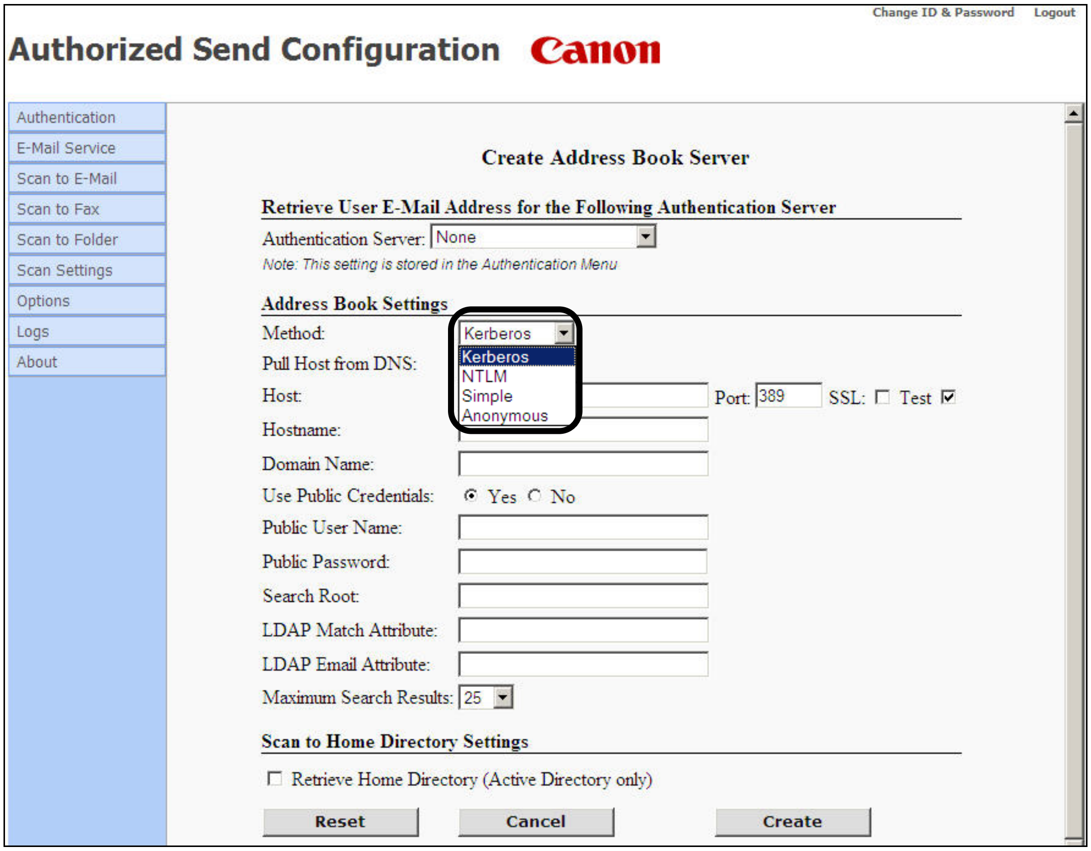
Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

NOTE

- The items in the Authentication Server drop-down list correspond to previously registered authentication servers.
- If you select [None] from the Authentication Server drop-down list, the address book server you create will not be associated with an authentication server and will not interact with any other features of Authorized Send. Select [None] if you want to create an address book server that can be configured at a later time.

3. Select the authentication method from the Method drop-down list.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: Kerberos

Pull Host from DNS:

Host: Port: 389 SSL: □ Test ☑

Hostname:

Domain Name:

Use Public Credentials: ● Yes ○ No

Public User Name:

Public Password:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

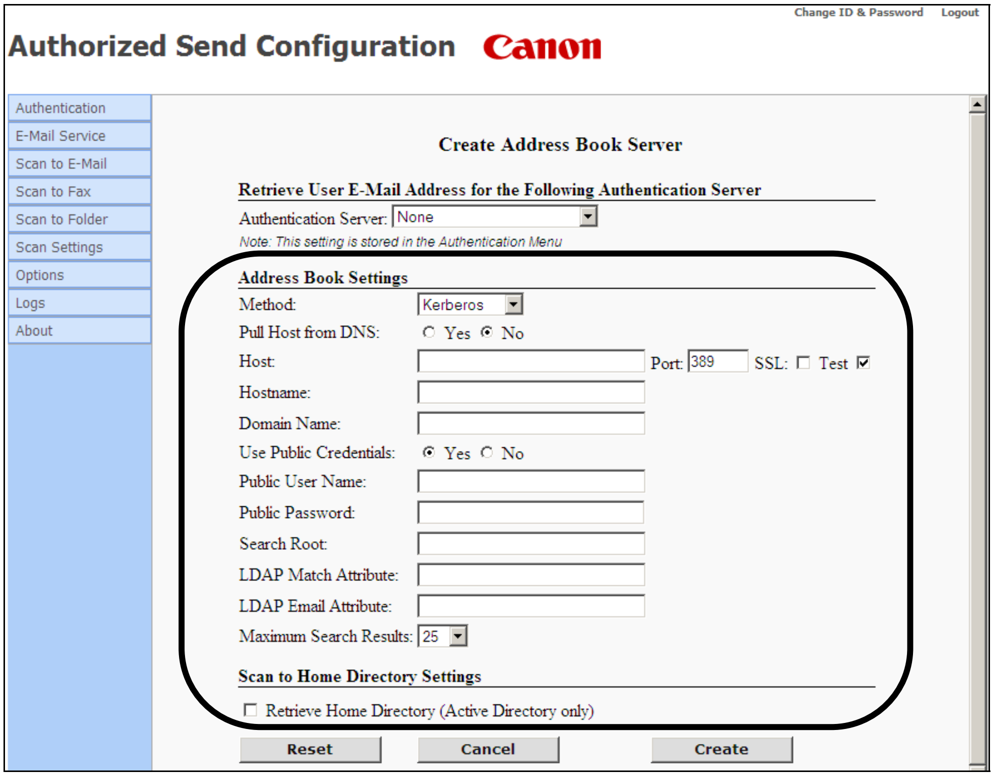
[Kerberos]: The machine communicates directly to Active Directory.

[NTLM]: The machine communicates directly to Active Directory.

[Simple]: Necessary, if you use Domino or eDirectory for authentication.

[Anonymous]: Authorized Send will not use any user login credentials to search the address book for e-mail addresses.

3.1 If you select [Kerberos] as the authentication method, specify the Address Book Settings and Scan to Home Directory Settings.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: Kerberos

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test ☑

Hostname:

Domain Name:

Use Public Credentials: ● Yes ○ No

Public User Name:

Public Password:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Address Book Settings

Method: Kerberos

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is ‘No’.

If you select the [Yes] radio button, the first “live” domain controller is used as the address book server after you click [Create].

Host: This text box is only displayed if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the address book server.

Port: This text box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: This check box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: This check box is only displayed if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.

Hostname: This text box is only displayed if Pull Host from DNS is set to ‘No’. Enter the host name of the address book server.

Domain Name: Enter the domain name of the address book server.

Pull Port from DNS: This check box is only displayed if Pull Host from DNS is set to ‘Yes’. Select the [Pull Port from DNS] check box if you want the Port text box to be dynamically populated from the DNS.

Use Public Credentials: Select [Yes] to use the public credentials (Public User Name and Public Password) configured by the System Administrator. Select [No] to use Anonymous binding.

Public User: This text box is only displayed if Use Public Credentials is

Name: set to ‘Yes’. It is used as the user name for authentication against the address book server. It is a required text box, with no limit on the number of characters that can be used.

Public Password: This text box is only displayed if Use Public Credentials is set to ‘Yes’. It is used as the password for authentication against the address book server. It is an optional text box, with no limit on the number of characters that can be used.

Search Root: Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.

LDAP Match Attribute: Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Retrieve Home Directory (Active Directory only] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.

An example for Active Directory is ‘sAMAccountName’ or ‘userPrincipalName’.

LDAP Email Attribute: Enter the e-mail LDAP attribute to pull the user’s e-mail address.

An example for Active Directory is ‘mail’.

Maximum Search Results: Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the ADDRESS BOOK screen of the machine. The default setting is ‘25’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user’s home directory information from the address book server with the LDAP attribute of “Home Directory.” This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

> IMPORTANT
>
> If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

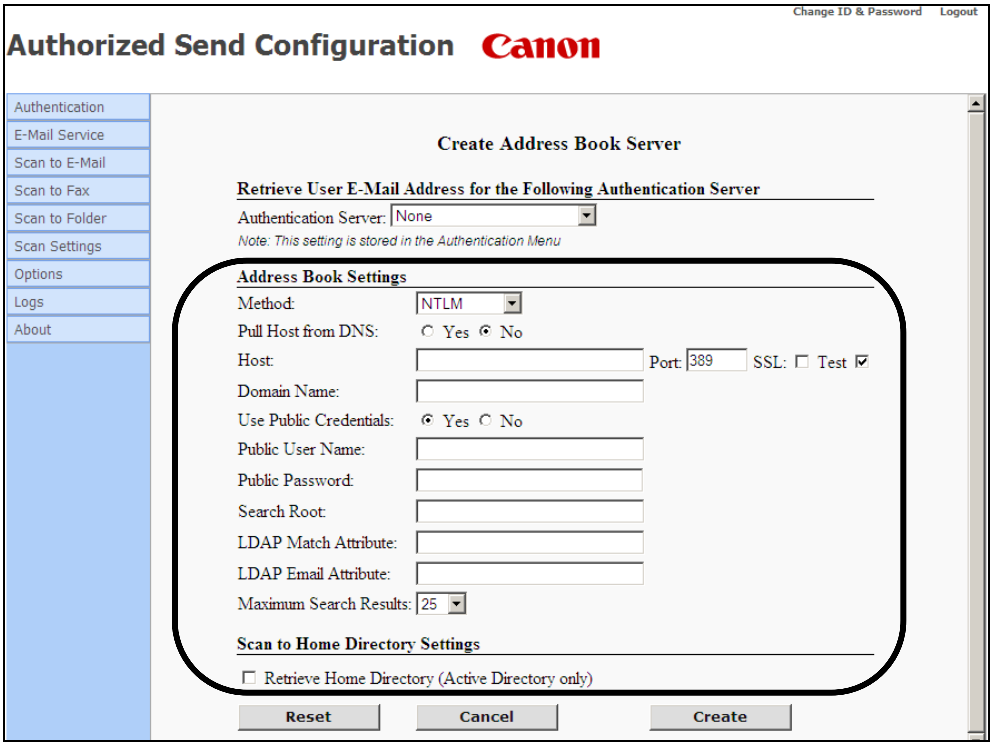
IMPORTANT

- If you select the Kerberos protocol for the authentication method, make sure that the device clock setting is properly synchronized with the configured authentication server and address book server. For more information on synchronizing the device clock with the server clock, see “Synchronizing the Device and Server Time,” on p. 142.
- Click the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message will be displayed. Enter the correct information ➞ click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

3.2 If you select [NTLM] as the authentication method, specify the Address Book Settings and Scan to Home Directory Settings.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: NTLM

Pull Host from DNS: ○ Yes ● No

Host: Port: 389 SSL: □ Test ☑

Domain Name:

Use Public Credentials: ● Yes ○ No

Public User Name:

Public Password:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Address Book Settings

Method:	NTLM

Pull Host from DNS: Select [Yes] to automatically pull the host information from the DNS after you click [Create]. Select [No] if you want to manually configure the host information. The default setting is ‘No’.

If you select the [Yes] radio button, the first “live” domain controller is used as the address book server after you click [Create].

Host: This text box is only displayed if Pull Host from DNS is set to ‘No’. Enter the DNS name or IP address of the address book server.

Port: This text box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.

SSL: This check box is only displayed if Pull Host from DNS is set to ‘No’ and if the [Pull Port from DNS] check box is not selected. Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.

Test: This check box is only displayed if Pull Host from DNS is set to ‘No’. Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.

Domain Name: This text box is only displayed if Pull Host from DNS is set to ‘No’. Enter the domain name of the address book server.

Pull Port from DNS: This check box is only displayed if Pull Host from DNS is set to ‘Yes’. Select the [Pull Port from DNS] check box if you want the Port text box to be dynamically populated from the DNS.

Use Public Credentials: Select [Yes] to use the public credentials (Public User Name and Public Password) configured by the System Administrator. Select [No] to use Anonymous binding.

Public User: This text box is only displayed if Use Public Credentials is

Name: set to ‘Yes’. It is used as the user name for authentication against the address book server. It is a required text box, with no limit on the number of characters that can be used.

Public Password: This text box is only displayed if Use Public Credentials is set to ‘Yes’. It is used as the password for authentication against the address book server. It is an optional text box, with no limit on the number of characters that can be used.

Search Root: Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.

LDAP Match Attribute:

Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Retrieve Home Directory (Active Directory only] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.

An example for Active Directory is ‘sAMAccountName’ or ‘userPrincipalName’.

LDAP Email Attribute:

Enter the e-mail LDAP attribute to pull the user’s e-mail address.

An example for Active Directory is ‘mail’.

Maximum Search Results:

Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the ADDRESS BOOK screen of the machine. The default setting is ‘25’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user’s home directory information from the address book server with the LDAP attribute of “Home Directory.” This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT

If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

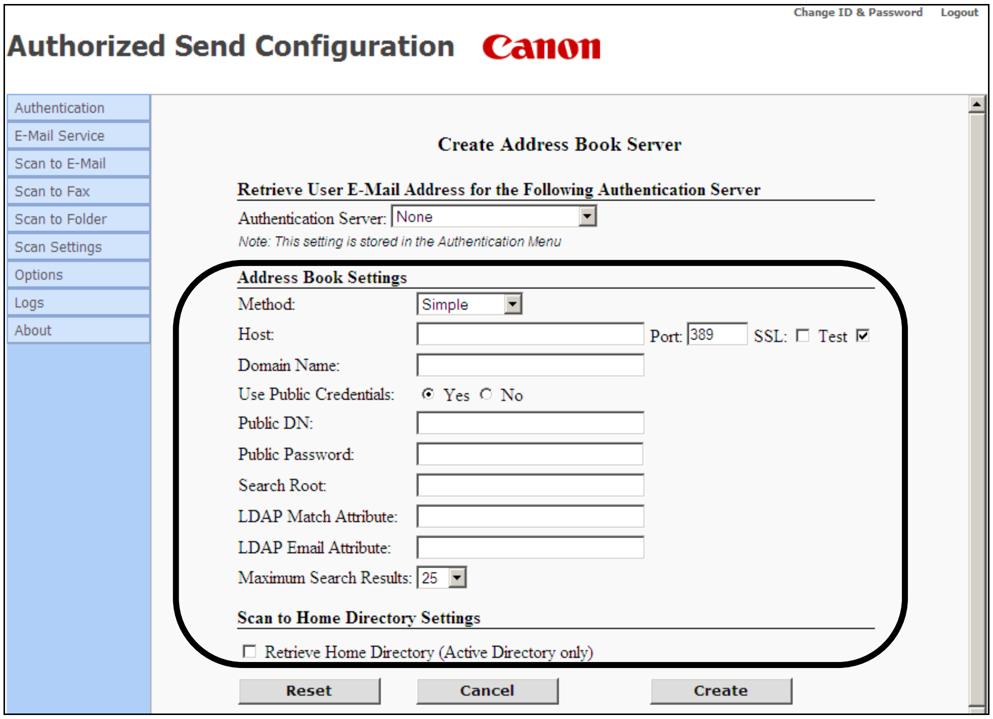
IMPORTANT

- Click the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message will be displayed. Enter the correct information → click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

3.3 If you select [Simple] as the authentication method, specify the Address Book Settings and Scan to Home Directory Settings.



Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: Simple

Host: Port: 389 SSL: □ Test ☑

Domain Name:

Use Public Credentials: ● Yes ○ No

Public DN:

Public Password:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Address Book Settings

Method:	Simple
Host:	Enter the DNS name or IP address of the address book server.
Port:	Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.
SSL:	Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.
Test:	Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.
Domain Name:	Enter the domain name of the address book server.

Use Public Credentials: Select [Yes] to configure the public credentials (Public DN and Public Password), or select [No] to use anonymous binding.

Public DN: This text box is only displayed if Use Public Credentials is set to 'Yes'. Enter the user's login Distinguished Name to use when performing the first bind of the Simple Binding process.

Public Password: This text box is only displayed if Use Public Credentials is set to 'Yes'. It is used as the password for authentication against the address book server. It is an optional text box, with no limit on the number of characters that can be used.

Search Root: Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.

LDAP Match Attribute: Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Retrieve Home Directory (Active Directory only] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.

An example for eDirectory and Domino is 'uid'.

LDAP Email Attribute: Enter the e-mail LDAP attribute to pull the user's e-mail address.

An example for eDirectory and Domino is 'mail'.

Maximum Search Results: Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the ADDRESS BOOK screen of the machine. The default setting is '25'.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user’s home directory information from the address book server with the LDAP attribute of “Home Directory.” This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

> IMPORTANT
>
> If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

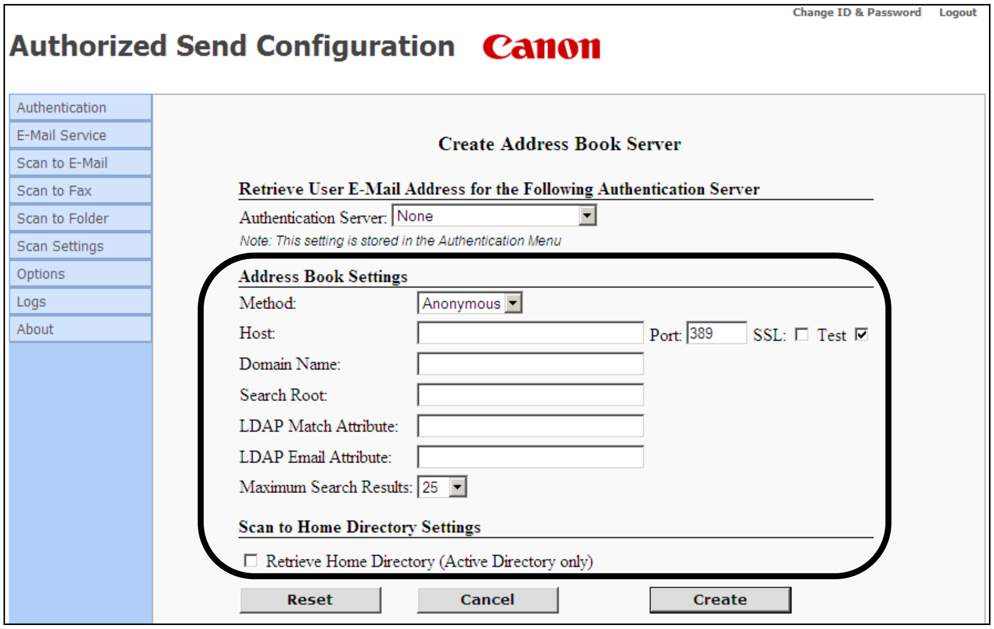
IMPORTANT

- Click the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message will be displayed. Enter the correct information ➞ click [Save].

NOTE

The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

3.4 If you select [Anonymous] as the authentication method, specify the Address Book Settings and Scan to Home Directory Settings.



Authorized Send Configuration

Create Address Book Server

Retrieve User E-Mail Address for the Following Authentication Server

Authentication Server: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: Anonymous

Host: Port: 389 SSL: □ Test ☑

Domain Name:

Search Root:

LDAP Match Attribute:

LDAP Email Attribute:

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

Address Book Settings

Method:	Anonymous
Host:	Enter the DNS name or IP address of the address book server.
Port:	Enter the connecting port number of the address book server. You can enter a maximum of five numbers. The default port number is ‘389’.
SSL:	Select this check box if you want the address book server to use SSL. If you select this check box, the host port number automatically changes to ‘636’.
Test:	Select this check box if you want the connection to the address book server to be verified before you save the settings. The [Test] check box is selected by default.
Domain Name:	Enter the domain name of the address book server.

Search Root: Depending on your environment, you must enter the Base DN (Distinguished Name) of the location of the user accounts.

If the directory server is authenticating against Active Directory and the domain is, for example, us.canon.com, then the search root is dc=us, dc=canon, dc=com.

If the directory server is authenticating against eDirectory or Domino and the organization is, for example, Canon, then the search root is o=canon.

LDAP Match Attribute: Enter the LDAP Match Attribute to be used for e-mail address retrieval. If the [Retrieve Home Directory (Active Directory only] check box is selected under <Scan to Home Directory Settings>, the value entered here is also used for Home Directory retrieval.

An example for Active Directory is ‘sAMAccountName’ or ‘userPrincipalName’.

An example for eDirectory and Domino is ‘uid’.

LDAP Email Attribute: Enter the e-mail LDAP attribute to pull the user’s e-mail address.

An example for Active Directory, eDirectory, and Domino is ‘mail’.

Maximum Search Results: Select [10], [25], [50], [75], or [100] from the drop-down list for the maximum number of search results that you want displayed on the ADDRESS BOOK screen of the machine. The default setting is ‘25’.

Scan to Home Directory Settings

Retrieve Home Directory (Active Directory only): Select this check box to obtain the currently logged on user’s home directory information from the address book server with the LDAP attribute of “Home Directory.” This will create a Home Directory element in the Preselected Share drop-down list on the Scan to Folder Preset Shares configuration screen.

IMPORTANT
If this check box is selected, and the [Retrieve Home Directory (Active Directory only] check box on the Create Authentication Server screen is also selected, the authentication server is checked first for the Home Directory. If no Home Directory is found on the authentication server, then the address book server is searched.

IMPORTANT

- Click the [Test] check box if you want to test the validity of the IP addresses you entered before saving.
- If validation fails, an error message will be displayed. Enter the correct information → click [Save].

NOTE
The [Test] check box is selected by default. If you do not want to test the validity of the addresses you entered, click the check box to clear the check mark.

4. Click [Create].

If you make a mistake while configuring the address book server settings, click [Reset] to return the settings to their original values.

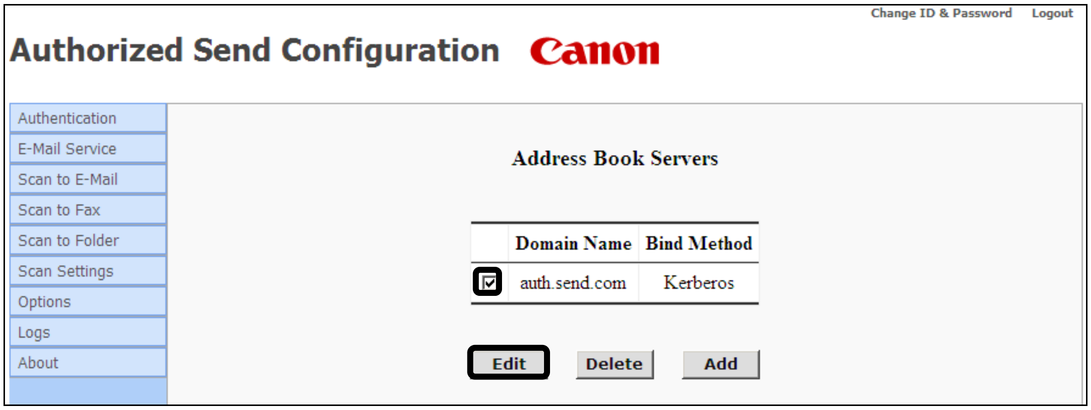
To cancel creating the address book server and return to the Address Book Servers screen, click [Cancel].

The address book server is created and added to the address book servers list on the Address Book Servers screen.

3.7 Editing an Address Book Server

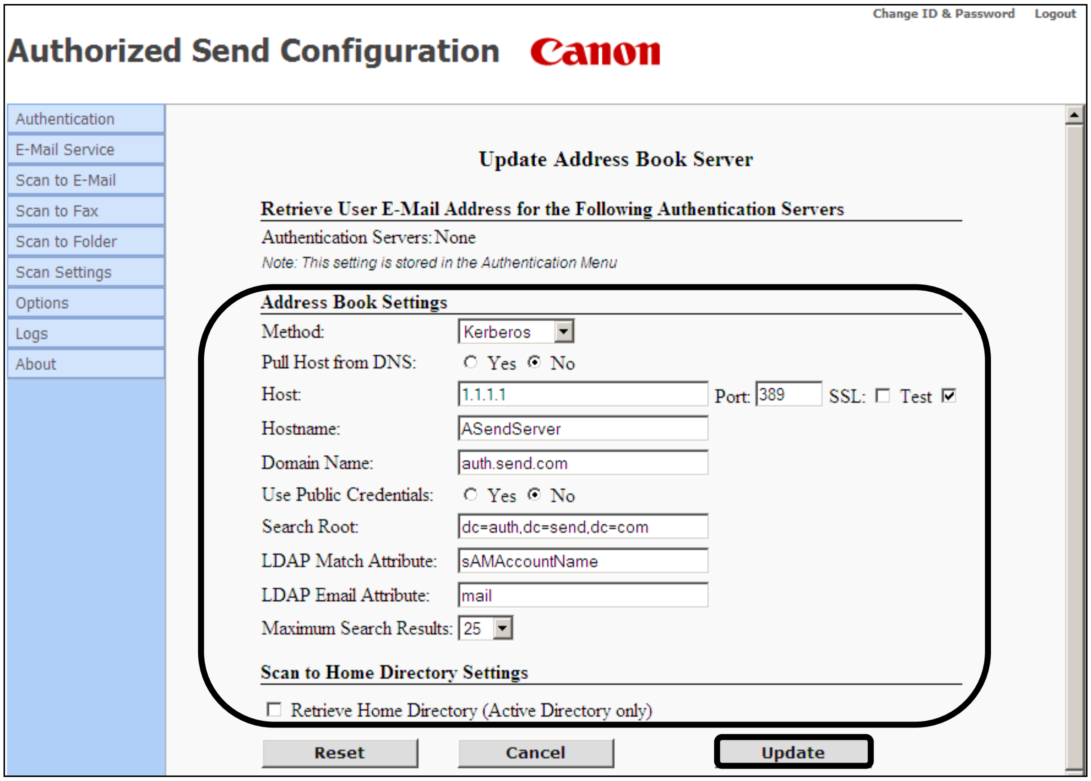
You can edit a previously created address book server from the Address Book Servers configuration screen.

1. Click [E-Mail Service] ➞ [Address Book] ➞ select the check box next to the address book server you want to edit ➞ click [Edit].



	Domain Name	Bind Method
☑	auth.send.com	Kerberos

2. Edit the settings for the address book server as necessary ➞ click [Update].



Update Address Book Server

Retrieve User E-Mail Address for the Following Authentication Servers

Authentication Servers: None

Note: This setting is stored in the Authentication Menu

Address Book Settings

Method: Kerberos

Pull Host from DNS: ○ Yes ● No

Host: 1.1.1.1 Port: 389 SSL: □ Test ☑

Hostname: ASendServer

Domain Name: auth.send.com

Use Public Credentials: ○ Yes ● No

Search Root: dc=auth,dc=send,dc=com

LDAP Match Attribute: sAMAccountName

LDAP Email Attribute: mail

Maximum Search Results: 25

Scan to Home Directory Settings

□ Retrieve Home Directory (Active Directory only)

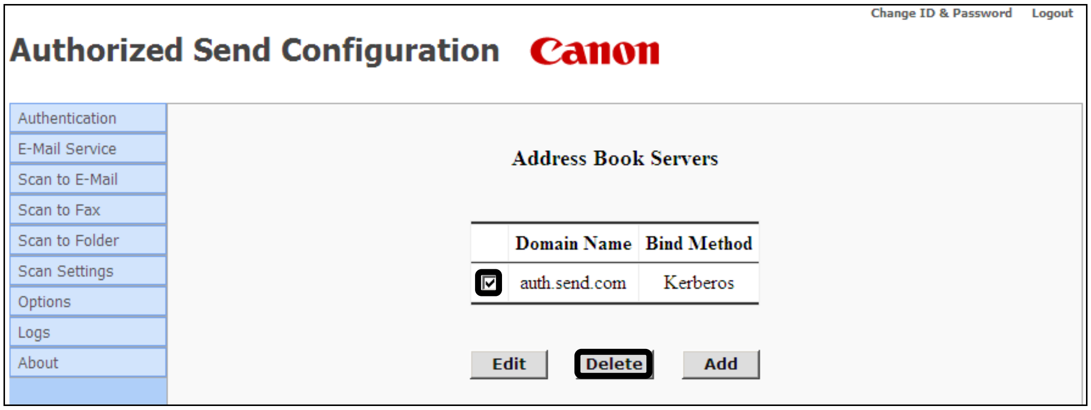
If you make a mistake while editing the address book server settings, click [Reset] to return the settings to their original values.

To cancel editing the address book server and return to the Address Book Servers screen, click [Cancel].

3.8 Deleting an Address Book Server

You can delete a previously created address book server from the Address Book Servers configuration screen.

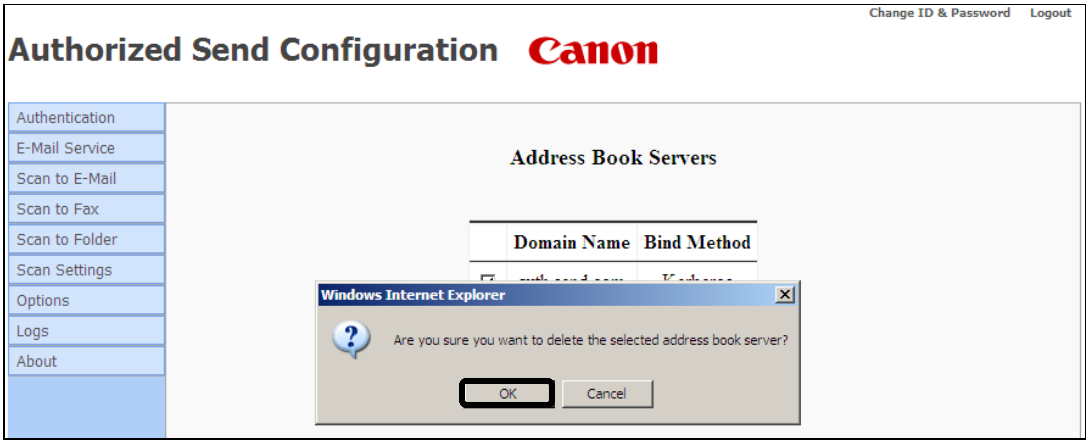
1. Click [E-Mail Service] ➞ [Address Book] ➞ select the check box next to the address book server you want to delete ➞ click [Delete].



Address Book Servers

	Domain Name	Bind Method
☑	auth.send.com	Kerberos

2. Click [OK].



Are you sure you want to delete the selected address book server?

If you do not want to delete the address book server, click [Cancel].

The address book server is deleted from the list.

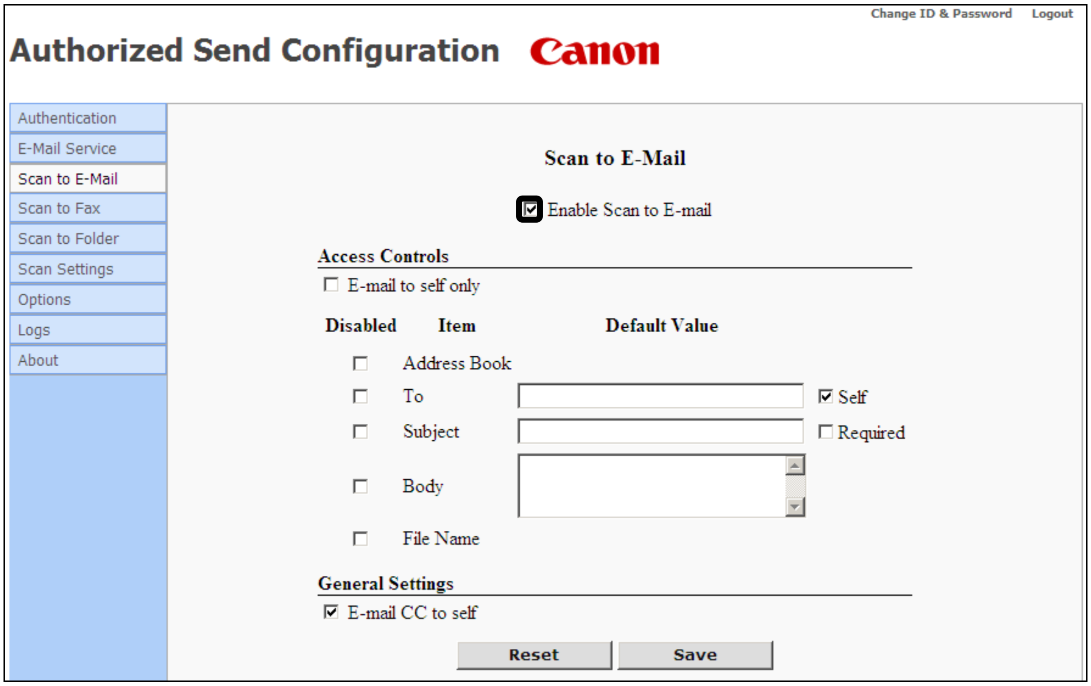
3.9 Configuring Scan to E-Mail Settings

You can enable the Scan to E-Mail function, restrict user access to the [Address Book] key and [To], [Subject], [Body], and [File Name] text boxes on the SCAN TO EMAIL screen on the machine, as well as enable E-mail CC to self.

1. Click [Scan to E-Mail].

   If necessary, see the screen shot in step 10 of "Flow of Configuration Operations," on p. 35.

2. Click the [Enable Scan to E-mail] check box.



Scan to E-Mail

☑ Enable Scan to E-mail

Access Controls

□ E-mail to self only

Disabled	Item	Default Value	
□	Address Book		
□	To		☑ Self
□	Subject		□ Required
□	Body		
□	File Name		

General Settings

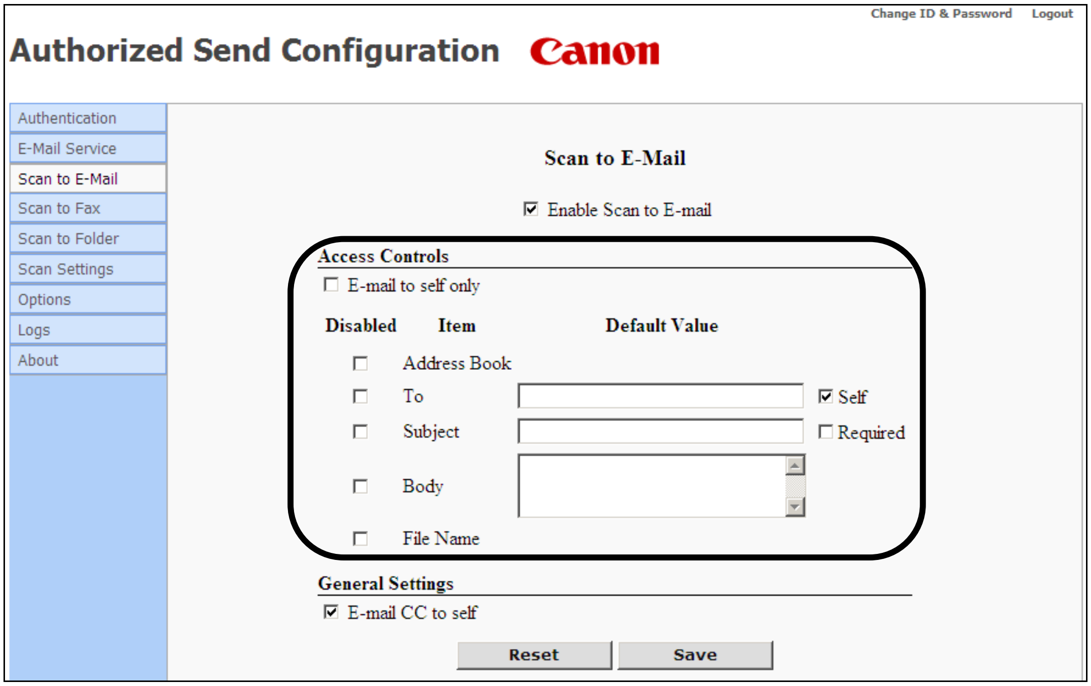
☑ E-mail CC to self

If you want to disable the Scan to E-Mail function, click the [Enable Scan to E-mail] check box to clear the check mark.

NOTE

You can only disable the Scan to E-Mail function if there is at least one other Authorized Send function enabled.

3. Configure the settings under <Access Controls>.



Authorized Send Configuration

Scan to E-Mail

☑ Enable Scan to E-mail

Access Controls

☐ E-mail to self only

Disabled	Item	Default Value	
☐	Address Book		
☐	To		☑ Self
☐	Subject		☐ Required
☐	Body		
☐	File Name		

General Settings

☑ E-mail CC to self

Access Controls

E-mail to self only: Select this check box if you want to restrict users to only send e-mail messages to themselves, and to automatically disable the [Address Book] key and the [To] text box on the SCAN TO EMAIL screen on the machine.

Disabled Column

Address Book: Select this check box if you want to restrict user access to the [Address Book] key on the SCAN TO EMAIL screen on the machine. If you select this check box, the [Address Book] key is not displayed on the SCAN TO EMAIL screen. The user can manually specify an e-mail address, but cannot select an address from the address book.

To: Select this check box if you want to prevent the user from manually entering an e-mail address. If you select this check box, the [To] text box on the SCAN TO EMAIL screen on the machine is grayed out. The user can select an e-mail address from the address book, but cannot manually specify an address.

Self

This check box is only displayed when the [E-mail to self only] check box is not selected. When the [Self] check box is selected, the e-mail address of the user logged on to Authorized Send is displayed in the [To] text box on the SCAN TO EMAIL Screen.

Subject:

Select this check box to disable the [Subject] text box on the SCAN TO EMAIL screen.

Required:

Select this check box if you require the user to enter a subject for their e-mail messages.

Body:

Select this check box to disable the [Body] text box on the SCAN TO EMAIL screen.

File Name:

Select this check box to disable the [File Name] text box on the SCAN TO EMAIL screen.

Default Value Column

To:

Enter the default e-mail address to be displayed in the [To] text box on the SCAN TO EMAIL screen.

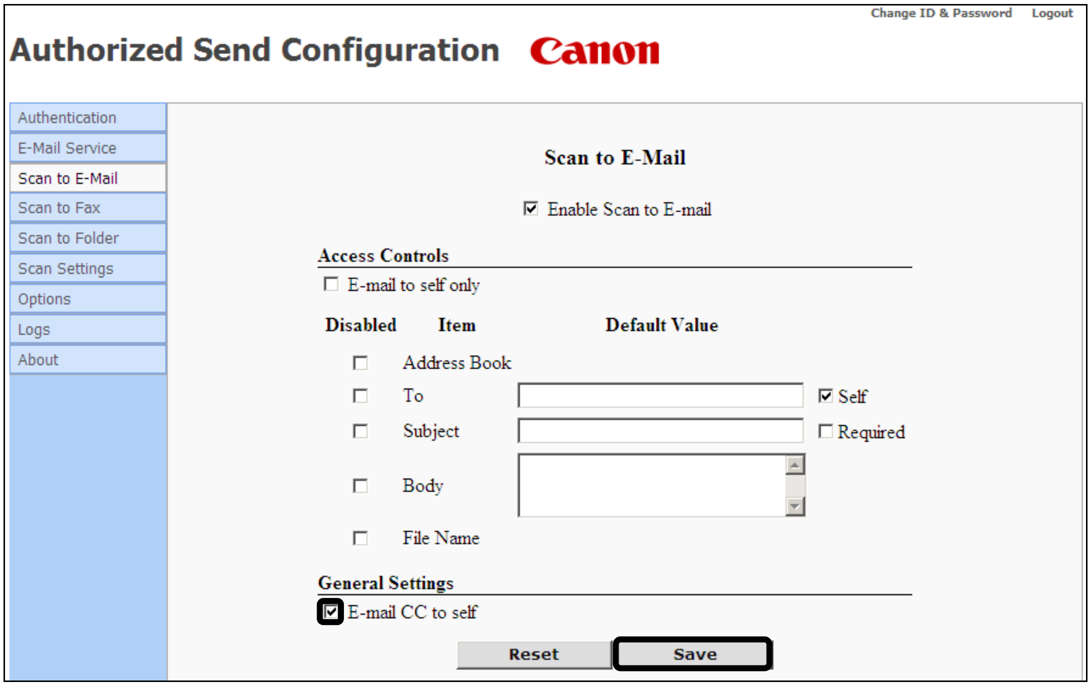
Subject:

Enter a default subject to be displayed in the [Subject] text box on the SCAN TO EMAIL screen.

Body:

Enter a default e-mail message to be displayed in the [Body] text box on the SCAN TO EMAIL screen.

4. If necessary, click the [E-mail CC to self] check box ➞ click [Save].



Authorized Send Configuration Canon

Scan to E-Mail

☑ Enable Scan to E-mail

Access Controls

☐ E-mail to self only

Disabled	Item	Default Value	
☐	Address Book		
☐	To		☑ Self
☐	Subject		☐ Required
☐	Body		
☐	File Name		

General Settings

☑ E-mail CC to self

If you select [E-mail CC to self], a copy of each e-mail message sent via SCAN TO EMAIL will be sent to the currently logged on user's e-mail address.

IMPORTANT

You must select the [Self] check box next to the [To] text box if you selected to disable the [Address Book] and [To] check boxes under <Disabled> at the same time, and the default value for the [To] text box is blank.

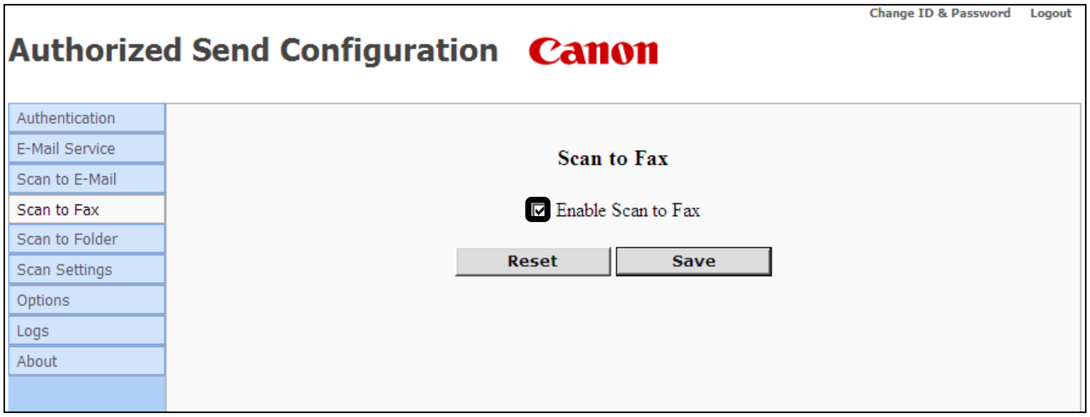
3.10 Configuring Scan to Fax Settings

You can enable the Scan to Fax function and configure the General Settings.

1. Click [Scan to Fax].

   If necessary, see the screen shot in step 12 of "Flow of Configuration Operations," on p. 35.

2. Click the [Enable Scan to Fax] check box.



Scan to Fax

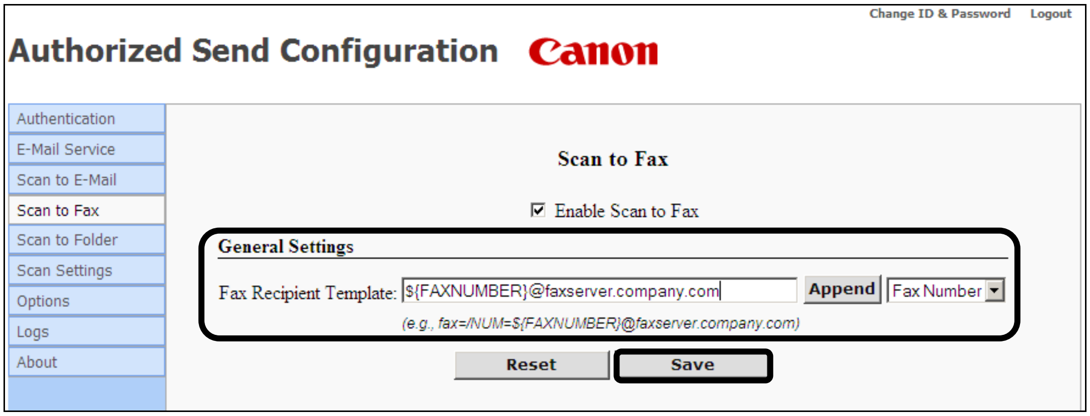
☑ Enable Scan to Fax

   If you want to disable the Scan to Fax function, click the [Enable Scan to Fax] check box to clear the check mark.

NOTE

- The Scan to Fax function is disabled by default.
- You can only disable the Scan to Fax function if there is at least one other Authorized Send function enabled.

3. Specify the General Settings ➞ click [Save].



Authorized Send Configuration

Scan to Fax

☑ Enable Scan to Fax

General Settings

Fax Recipient Template: ${FAXNUMBER}@faxserver.company.com Fax Number

(e.g., fax=/NUM=${FAXNUMBER}@faxserver.company.com)

General Settings

Fax Recipient Template: Enter the appropriate template configuration.

For example, if you enter **${FAXNUMBER}@faxserver.company.com** as the string, and the fax number entered by the user (for example, '1234567') when sending from the Scan to Fax screen, Authorized Send sends an e-mail message to the SMTP server with "1234567@faxserver.company.com" in the "To:" text box.

Append: Clicking [Append] appends a dynamic variable (set in the Append drop-down list) to the string in the Fax Recipient Template. This is unnecessary if the string is entered manually in the [Fax Recipient Template] text box.

Append drop-down: Selecting [Fax Number] in conjunction with pressing [Append] adds the fax number variable '${FAXNUMBER}' to the string in the [Fax Recipient Template] text box.

NOTE

- The user does not see the template. The user only has to enter the fax number(s) on the Authorized Send SCAN TO FAX screen on the machine.
- If you upgrade Authorized Send from version 3.x to 4.0 or later, the fax template is automatically updated to the current format, which would include: '${FAXNUMBER}' as the prefix to what was configured in version 3.x.

  For example, if the Domain text box on the Scan to Fax screen of the Authorized Send Configuration servlet was configured with "auth.send.com" in Authorized Send v3.x, when upgrading to Authorized Send v4.0 or later, the Fax Recipient Template text box on the Scan to Fax screen of the Authorized Send Configuration servlet is configured with '${FAXNUMBER}@auth.send.com'.

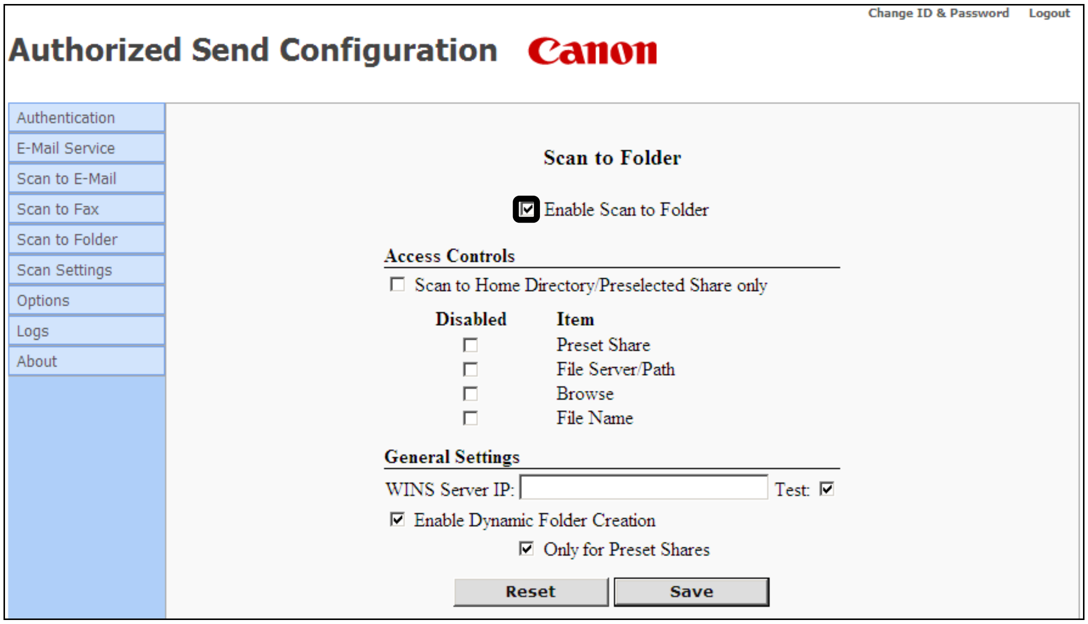
3.11 Configuring Scan to Folder Settings

You can enable the Scan to Folder function and configure the Access Controls and General Settings.

1. Click [Scan to Folder] ➞ [General].

   If necessary, see the screen shot in step 14 of "Flow of Configuration Operations," on p. 35.

2. Select the [Enable Scan to Folder] check box.



Scan to Folder

☑ Enable Scan to Folder

Access Controls

□ Scan to Home Directory/Preselected Share only

Disabled	Item
□	Preset Share
□	File Server/Path
□	Browse
□	File Name

General Settings

WINS Server IP: Test: ☑

☑ Enable Dynamic Folder Creation

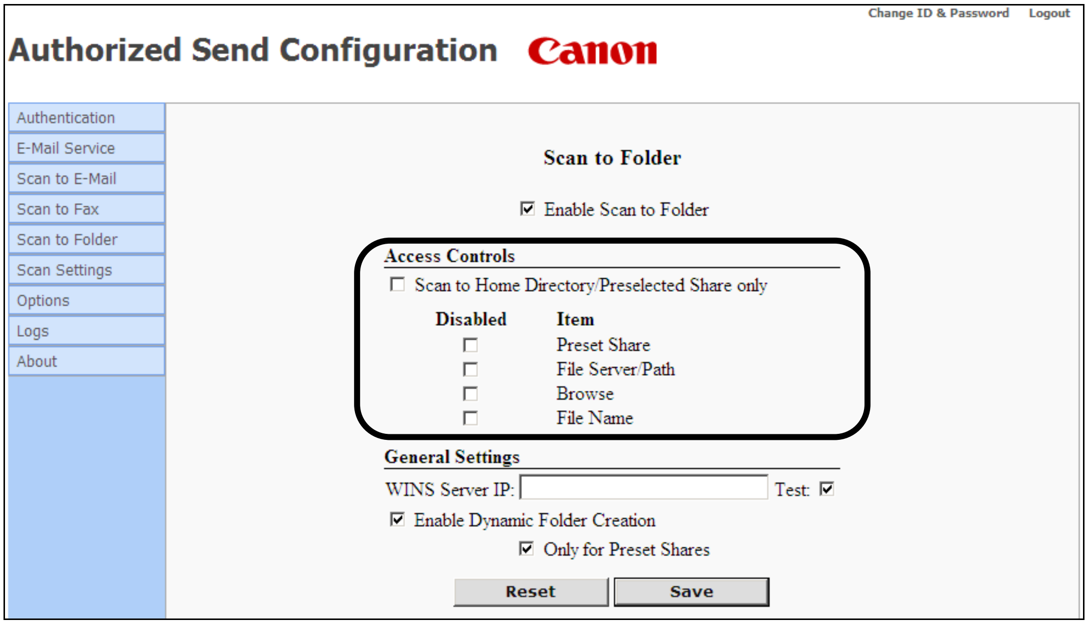
☑ Only for Preset Shares

If you want to disable the Scan to Folder function, click the [Enable Scan to Folder] check box to clear the check mark.

NOTE

You can only disable the Scan to Folder function if there is at least one other Authorized Send function enabled.

3. Configure the settings under <Access Controls>.



Scan to Folder

☑ Enable Scan to Folder

Access Controls

□ Scan to Home Directory/Preselected Share only

Disabled	Item
□	Preset Share
□	File Server/Path
□	Browse
□	File Name

General Settings

WINS Server IP: Test: ☑

☑ Enable Dynamic Folder Creation

☑ Only for Preset Shares

Access Controls

Scan to Home Directory/Preselected Share only: Select this check box if you want to automatically disable the [Preset Share], [File Server/Path], and [Browse] check boxes with one click.

Disabled Column

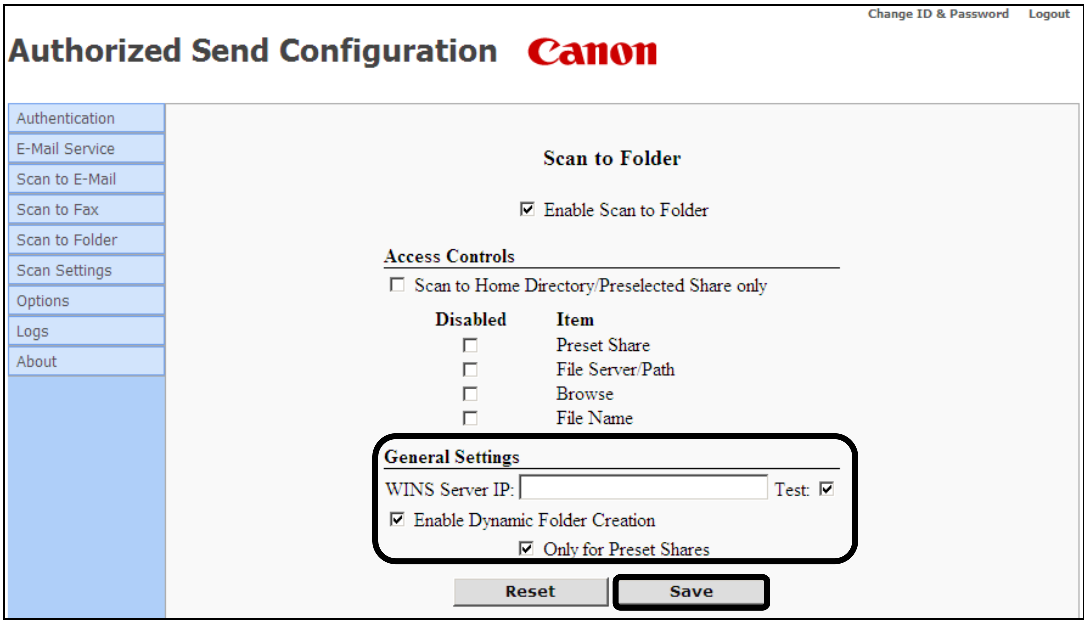
Preset Share: Select this check box if you want to prevent the user from selecting a preset share from the Preset Share drop-down list on the SCAN TO FOLDER screen. If you select this check box, the Preset Share drop-down list is grayed out.

File Server/Path: Select this check box if you want to disable the [File Server] and [File Path] text boxes on the SCAN TO FOLDER screen. If you select this check box, the [File Server] and [File Path] text boxes are grayed out.

Browse: Select this check box if you want to disable the [Browse] button on the SCAN TO FOLDER screen. If you select this check box, the [Browse] button does not appear on the SCAN TO FOLDER screen.

File Name: Select this check box if you want to prevent the user from using the [File Name] text box on the SCAN TO FOLDER screen. If you select this check box, the [File Name] text box is grayed out.

4. Specify the General Settings ➞ click [Save].



Scan to Folder

☑ Enable Scan to Folder

Access Controls

☐ Scan to Home Directory/Preselected Share only

Disabled	Item
☐	Preset Share
☐	File Server/Path
☐	Browse
☐	File Name

General Settings

WINS Server IP: Test: ☑

☑ Enable Dynamic Folder Creation

☑ Only for Preset Shares

General Settings

WINS Server IP: Enter the IP address of the NetBIOS name server.

Test: Select this check box if you want the connection to the WINS server to be verified before you save the settings. The [Test] check box is selected by default.

Enable Dynamic Folder Creation: Select this check box to automatically create any folders in the share path that may not exist when a user scans a document.

Only for Preset Shares: Select this check box to enable dynamic folder creation for preset shares created only by a System Administrator. If a user enters a share path manually that does not exist, the share is not dynamically created when a user scans a document.

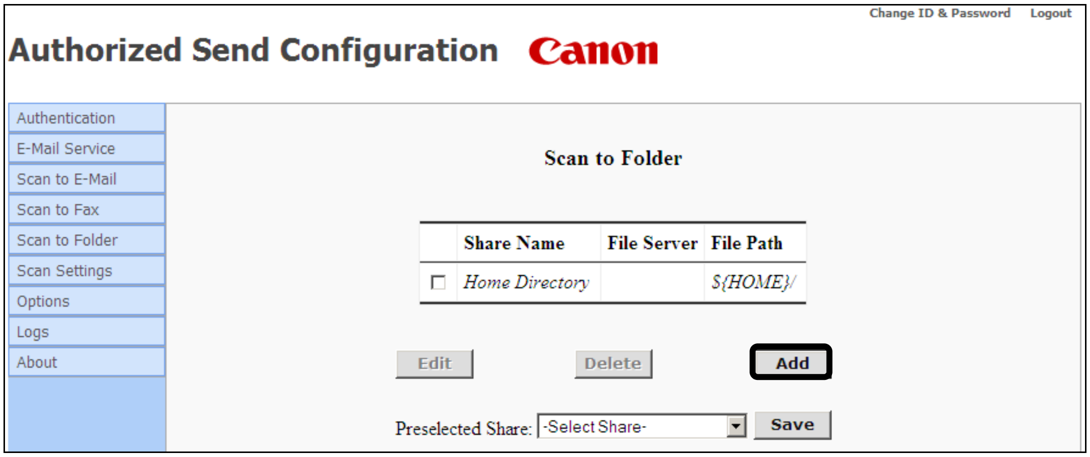
3.12 Creating a Preset Share

You can create any number of preset shares.

1. Click [Scan to Folder] ➞ [Preset Shares].

   If necessary, see the screen shot in step 16 of “Flow of Configuration Operations,” on p. 35.

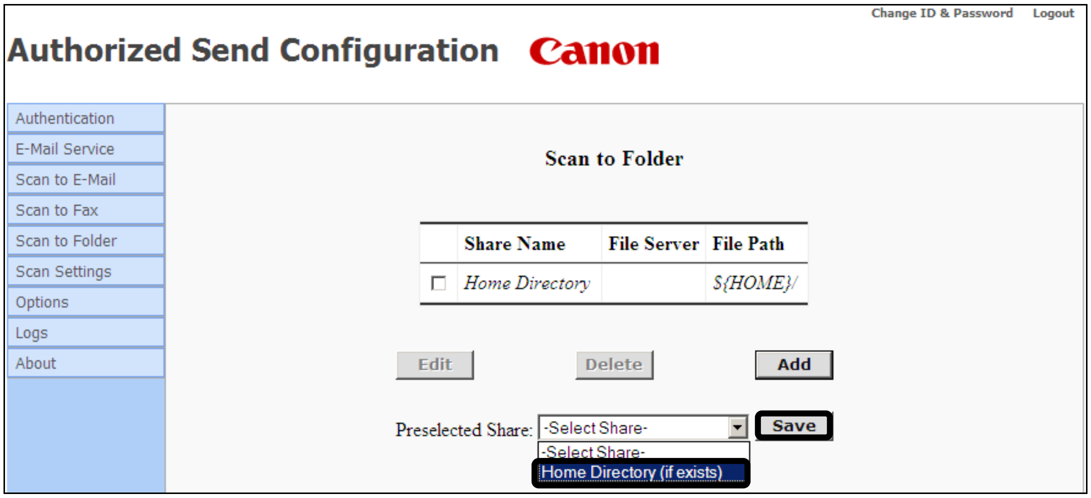
2. Click [Add].



	Share Name	File Server	File Path
□	*Home Directory*		*${HOME}/*

Preselected Share: -Select Share-

If you want to specify your home directory as a preselected share that will automatically appear in the Preset Share drop-down list on the SCAN TO FOLDER screen, select [Home Directory (if exists)] from the Preselected Share drop-down list ➞ click [Save].



Scan to Folder

	Share Name	File Server	File Path
□	*Home Directory*		*${HOME}/*

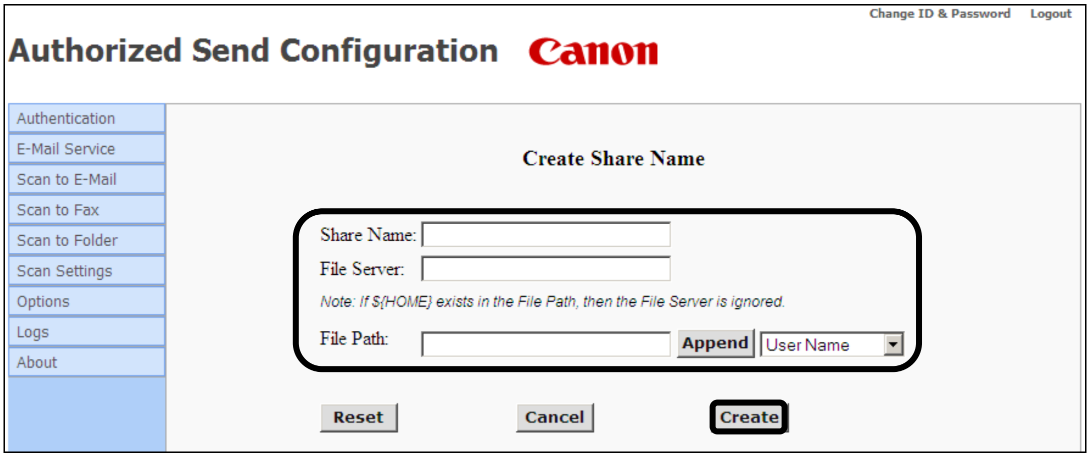
Preselected Share: -Select Share-

-Select Share-
Home Directory (if exists)

NOTE

If you do not have a Home Directory, or if you do not select [Home Directory (if exists)] from the Preselected Share drop-down list, no share will appear on the SCAN TO FOLDER screen.

3. Specify the Share Name settings ➞ click [Create].



Note: If ${HOME} exists in the File Path, then the File Server is ignored.

Create Share Name

Share Name: Enter a name for the preset share. The Share Name is case-sensitive. You can enter a maximum of 31 characters.

File Server: Enter the DNS name or IP Address to send documents.

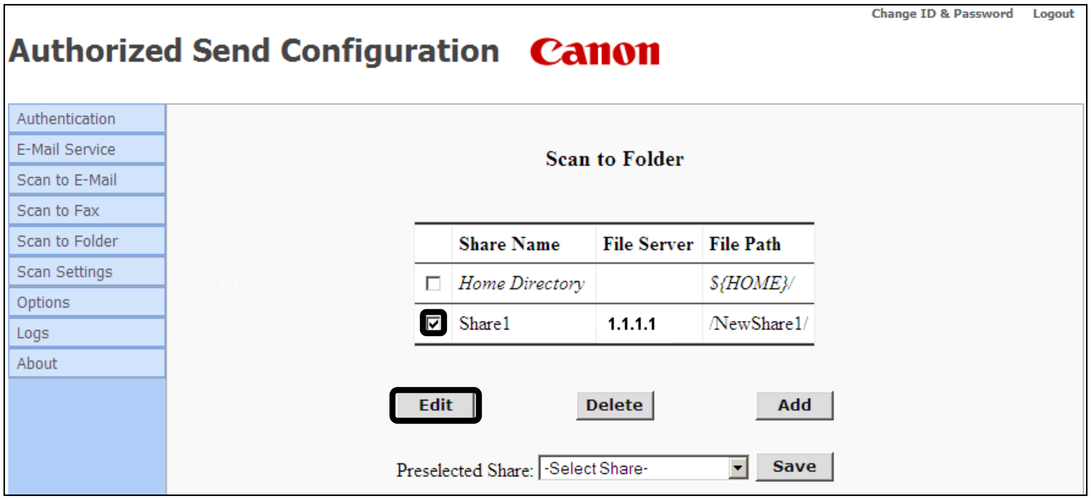
File Path: Enter the path of the folder to send documents.

Append: Click [Append] to add a user’s name to the string in the [File Path] text box.

3.13 Editing a Preset Share

You can edit a previously created preset share from the Scan to Folder configuration screen.

1. Click [Scan to Folder] ➞ [Preset Shares] ➞ select the check box next to the preset share you want to edit ➞ click [Edit].

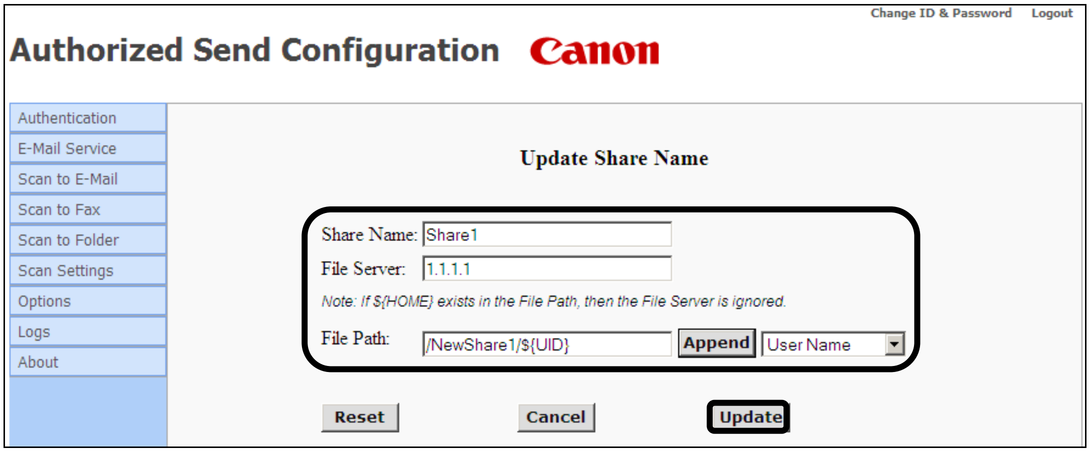


Scan to Folder

	Share Name	File Server	File Path
□	*Home Directory*		*${HOME}/*
☑	Share1	1.1.1.1	/NewShare1/

Preselected Share: -Select Share-

2. Edit the settings for the preset share as necessary ➞ click [Update].



Update Share Name

Share Name: Share1

File Server: 1.1.1.1

Note: If ${HOME} exists in the File Path, then the File Server is ignored.

File Path: /NewShare1/${UID} User Name

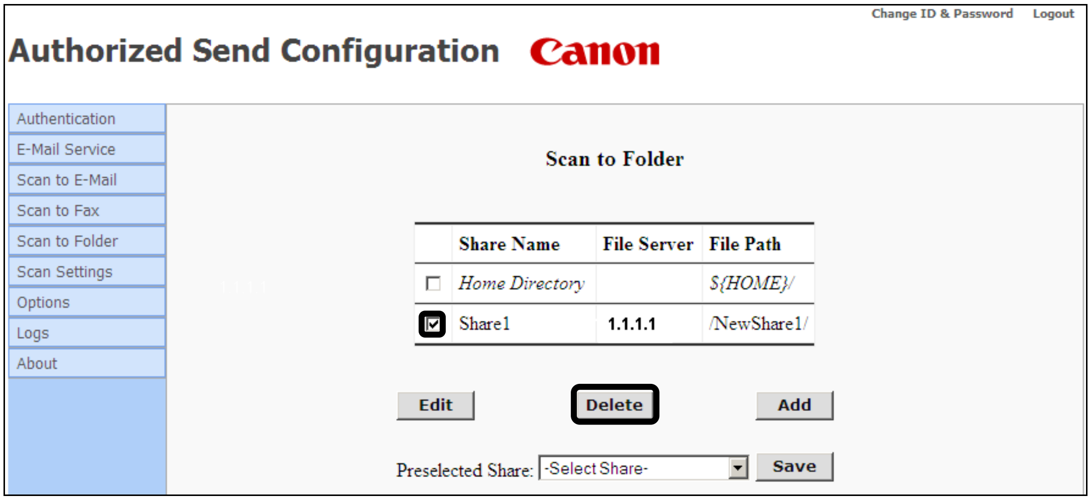
If you make a mistake, click [Reset] to return the settings to their original values.

To cancel editing the preset share and return to the Scan to Folder configuration screen, click [Cancel].

3.14 Deleting a Preset Share

You can delete a previously created preset share from the Scan to Folder configuration screen.

1. Click [Scan to Folder] ➞ [Preset Shares] ➞ select the check box next to the preset share you want to delete ➞ click [Delete].



	Share Name	File Server	File Path
□	*Home Directory*		*${HOME}/*
☑	Share1	1.1.1.1	/NewShare1/

Preselected Share: -Select Share-

2. Click [OK] on the confirmation dialog box.

   If you do not want to delete the preset share, click [Cancel].

   The preset share is deleted from the list.

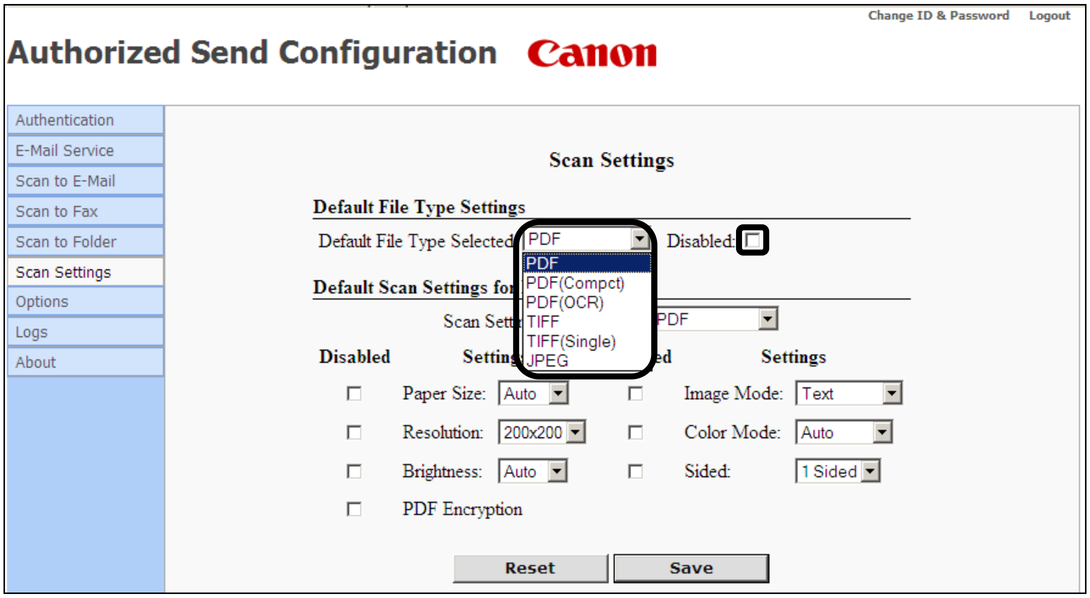
3.15 Configuring Scan Settings

You can configure the Default File Type Settings and Default Scan Settings For File Types. This causes the default scan settings to automatically change based on the file type that is selected.

1. Click [Scan Settings].

   If necessary, see the screen shot in step 18 of "Flow of Configuration Operations," on p. 35.

2. Specify the Default File Type Settings.



Scan Settings

Default File Type Settings

Default File Type Selected: PDF — Disabled: □

PDF
PDF(Compct)
PDF(OCR)
TIFF
TIFF(Single)
JPEG

Default Scan Settings for

Scan Sett... PDF

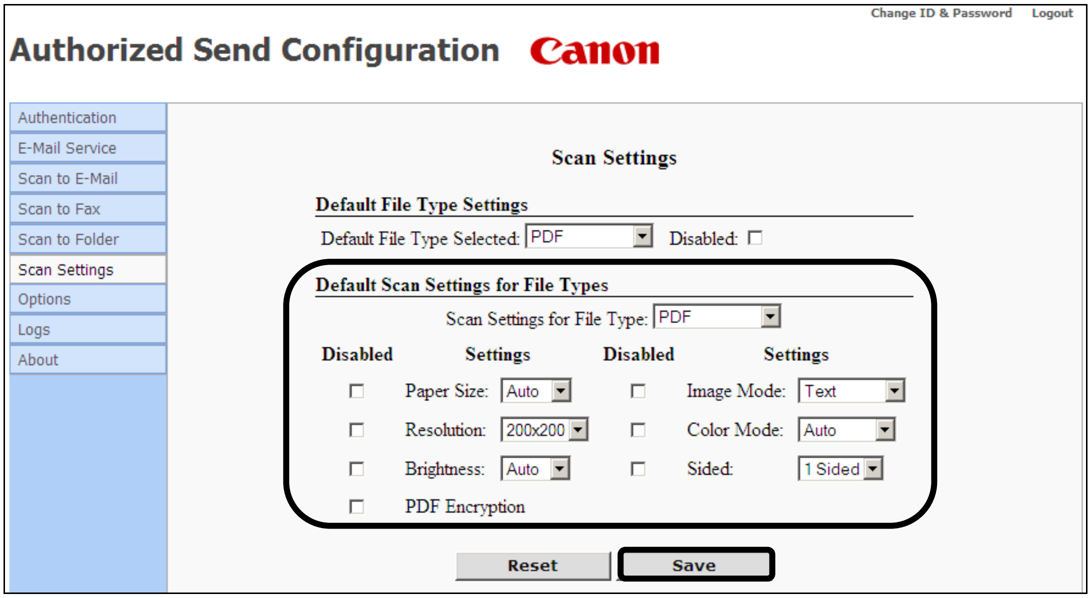
Disabled	Settings		Disabled	Settings	
□	Paper Size:	Auto	□	Image Mode:	Text
□	Resolution:	200x200	□	Color Mode:	Auto
□	Brightness:	Auto	□	Sided:	1 Sided
□	PDF Encryption				

Default File Type Settings

Default File Type Selected: If want to change the default file type, select a file type from the drop-down list. The default Default File Type Selected is 'PDF'.

Disabled: Select this check box if you want to disable and gray out the File Type drop-down list on the SCAN SETTINGS screen.

3. Configure the settings under <Default Scan Settings for File Types> ➞ click [Save].



Authorized Send Configuration Canon

Scan Settings

Default File Type Settings

Default File Type Selected: PDF Disabled: □

Default Scan Settings for File Types

Scan Settings for File Type: PDF

Disabled	Settings		Disabled	Settings	
□	Paper Size:	Auto	□	Image Mode:	Text
□	Resolution:	200x200	□	Color Mode:	Auto
□	Brightness:	Auto	□	Sided:	1 Sided
□	PDF Encryption				

Default Scan Settings for File Types

Scan Settings for File Type: Select [PDF], [PDF(Compct)], [PDF(OCR)], [TIFF], [TIFF(Single)], or [JPEG] from the drop-down list. This file type in conjunction with the specific scan settings that you select and save, are displayed as the new default settings for that file type on the SCAN SETTINGS screen. The default Scan Settings for File Type is 'PDF'.

Disabled Column By default, each check box in this column is not selected unless a particular default scan setting, which is based on the file type selected from the Scan Settings for File Type drop-down list, requires it to be disabled and grayed out.

Paper Size: Select this check box to disable and gray out the Paper Size drop-down list on the SCAN SETTINGS screen.

Resolution: Select this check box to disable and gray out the Resolution drop-down list on the SCAN SETTINGS screen.

Brightness: Select this check box to disable and gray out the Brightness scroll bar on the SCAN SETTINGS screen.

PDF Encryption: Select this check box to hide the PDF Encryption icon on the SCAN SETTINGS screen.

NOTE

The PDF Encryption check box only appears on machines that support PDF encryption.

Image Mode: Select this check box to disable and gray out the Image Mode drop-down list on the SCAN SETTINGS screen.

Color Mode: Select this check box to disable and gray out the Color Mode drop-down list on the SCAN SETTINGS screen.

Sided: Select this check box to disable and gray out the Document check box on the SCAN SETTINGS screen.

Settings Column By default, some settings are automatically selected and grayed out, based on the file type selected from the Scan Settings for File Type drop-down list.

Paper Size: Select [Auto], [Letter], [Legal], or [11x17] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default Paper Size is ‘Auto’.

NOTE

- Select [Letter] if you want to scan in a portrait orientation.
- If you select [Letter] for scanning in a landscape orientation, the scanned image is truncated.
- Select [Auto] if you want to scan a letter-size document in a landscape orientation.
- If [Auto] is selected, scanning originals with different sizes or with different orientations may produce unexpected results.

Resolution:

Select [200x200], [300x300], or [600x600] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default Resolution depends on the file type that you selected.

NOTE

- If your machine does not support a particular resolution, that resolution is not displayed.
- Authorized Send Version 4.0 and lower versions have a ‘DPI is user Configurable’ setting on the Options screen in the Configuration servlet. This allows the System Administrator to enable or disable the resolution on the SCAN SETTINGS screen for the end user. However, this setting has been removed from Authorized Send Version 4.1, since the resolution enable or disable state is now configured on the Scan Settings screen in the Configuration servlet.
- If the [DPI is user Configurable] check box was not selected and an upgrade to Authorized Send Version 4.1 is performed, the resolution is disabled for all file types.

Brightness:

Select [Auto], [10%], [20%], [30%], [40%], [50%], [60%], [70%], [80%], [90%], or [100%] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default Brightness is ‘Auto’.

PDF Encryption:

The default setting is for the PDF Encryption icon to appear on the SCAN SETTINGS screen. PDF encryption is available only for PDF, PDF(Compct), and PDF(OCR) file types.

Image Mode:

Select [Text], [Text/Photo], or [Photo] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default Image Mode is ‘Text’.

Color Mode: Select [Auto], [Full Color], or [Black] from the drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default Color Mode depends on the file type that you selected.

NOTE

- If your machine is black-and-white only, [Black] is automatically selected and the Color Mode drop-down list is disabled and grayed out.
- The Color Mode selections that are available depend on the file type that you selected from the Scan Settings for File Type drop-down list.

– PDF:	[Auto], [Full Color], and [Black]
– PDF(Compct):	[Full Color]
– PDF(OCR):	[Auto], [Full Color], and [Black]
– TIFF:	[Black]
– TIFF(Single):	[Black]
– JPEG:	[Full Color]

Sided: Select [1-Sided] or [2-Sided] from this drop-down list to correspond with the file type that you selected from the Scan Settings for File Type drop-down list. The default Sided is ‘1 Sided’.

NOTE

The table below displays the default scan settings for each file type that automatically appears on the SCAN SETTINGS screen on the machine, unless they are changed and saved by the System Administrator.

File Type	**Paper Size**	**Res.**	**Bright.**	**PDF Encrypt.**	**Img. Mode**	**Color Mode**	**Sided**
PDF	Auto	200x200	Auto	Available	Text	Auto	1 Sided
PDF(Compct)	Auto	300x300*1	Auto	Available	Text	Full Color*2	1 Sided
PDF(OCR)	Auto	200x200	Auto	Available	Text	Auto	1 Sided
TIFF	Auto	200x200	Auto	Not Available	Text	Black*2	1 Sided
TIFF(Single)	Auto	200x200	Auto	Not Available	Text	Black*2	1 Sided
JPEG	Auto	200x200	Auto	Not Available	Text	Full Color*2	1 Sided

*1 The Resolution Mode drop-down list is disabled.

*2 The Color Mode drop-down list is disabled.

3.16 Configuring Optional Settings

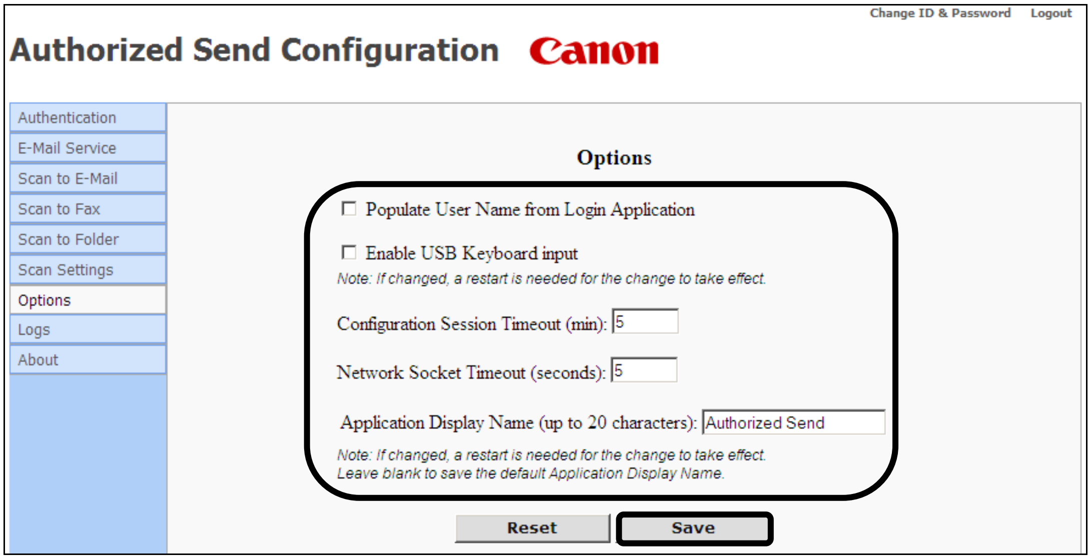
You can configure the timeout settings, decide whether to populate the User Name text box on the Authorized Send SIGN IN screen, enable USB keyboard input, and rename the tab of the Authorized Send application on the machine.

IMPORTANT
You can use third-party USB keyboards with Authorized Send. However, only the Cherry G84 keyboard has been tested with this application.

1. Click [Options].

   If necessary, see the screen shot in step 20 of "Flow of Configuration Operations," on p. 35.

2. Specify the settings on the Options screen as necessary ➞ click [Save].



Options

☐ Populate User Name from Login Application

☐ Enable USB Keyboard input

Note: If changed, a restart is needed for the change to take effect.

Configuration Session Timeout (min): 5

Network Socket Timeout (seconds): 5

Application Display Name (up to 20 characters): Authorized Send

Note: If changed, a restart is needed for the change to take effect.
Leave blank to save the default Application Display Name.

Options

Populate User Name from Login Application:	Select this check box to have the [User Name] text box on the Authorized Send SIGN IN screen automatically populated with the user's name from the machine's login application (if used). If no login application is used, the user must enter their log on name manually.

Enable USB Keyboard input:

Select this check box to enable your machine to utilize an attached USB keyboard. If this check box is not selected, your machine cannot utilize an attached USB keyboard and automatically uses the MEAP virtual keyboard instead. If you select the [Enable USB Keyboard input] check box, the [Only Use Cherry G84 Keyboard] check box is selected automatically. The [Enable USB Keyboard input] check box is not selected by default.

NOTE

- If a USB keyboard is attached to or detached from the machine after Authorized Send has been installed and started, the machine must be restarted.
- imageRUNNERs 3225/3230/3235/3245 have a setting to enable or disable the MEAP driver for USB input. This setting must be turned on to use the USB keyboard with Authorized Send. To turn this setting on, go to the machine’s control panel, press ⊛ (Additional Functions) ➞ [System Settings] ➞ [USB Settings] ➞ [Use MEAP Driver for USB Input Device] ➞ select [On].
- If the [Enable USB Keyboard input] check box is selected and the machine is restarted, you will only be able to use an attached USB keyboard to input text. If no USB keyboard is attached, you have no way to input text into Authorized Send since the MEAP virtual keyboard is not displayed.
- The machine must be restarted each time you select or clear the [Enable USB Keyboard input] check box for the change to take effect.

Only Use Cherry G84 Keyboard:

Select this check box if you want to only use the Cherry G84 keyboard. By default, this check box is selected.

NOTE

- The [Only Use Cherry G84 Keyboard] check box is displayed only if the [Enable USB Keyboard input] check box is selected.
- If a Cherry G84 keyboard and another HID are connected to your machine at the same time, only the Cherry G84 keyboard is functional for Authorized Send.
- If the [Only Use Cherry G84 Keyboard] check box is not selected and a non-keyboard HID is the only device connected to your machine, you have no way to input text into Authorized Send since the MEAP virtual keyboard is not displayed.
- If the [Only Use Cherry G84 Keyboard] check box is not selected and the [Enable USB Keyboard input] check box is selected, any USB keyboard can be used to input text, but only the Cherry G84 keyboard is supported. In this case, to avoid any incompatibility issues between MEAP installed applications and HID card readers, or other HIDs, it is recommended that you select the [Only Use Cherry G84 Keyboard] check box.
- The machine must be restarted each time you select or clear the [Only Use Cherry G84 Keyboard] check box for the change to take effect.

Configuration Session Timeout (min):

Enter the time in minutes until the Authorized Send Configuration servlet session times out. You can set the timeout period between ‘1’ and ‘60’ minutes. The default setting is ‘5’ minutes.

Network Socket Timeout (seconds):

Enter the time in seconds until the connection to the authentication server and address book server times out. You can set the timeout period between ‘1’ and ‘30’ seconds. The default setting is ‘5’ minutes.

Application Display Name (up to 20 characters):

Enter the application display name. You can enter a maximum of 20 characters. Valid characters are the printable ASCII characters and the carriage return. The default setting is ‘Authorized Send’.

If the application display name is changed, restart the machine for the change to take effect. If you want to return to the default setting, leave this text box blank.

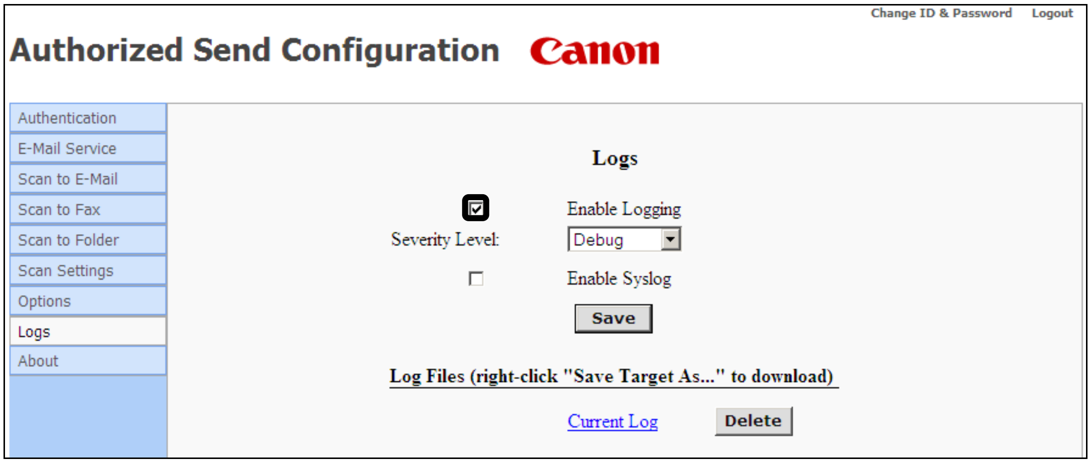
3.17 Configuring Log Settings

You can enable the Log function and view or delete the current log file.

1. Click [Logs].

   If necessary, see the screen shot in step 22 of “Flow of Configuration Operations,” on p. 35.

2. Click the [Enable Logging] check box.



Logs

☑ Enable Logging

Severity Level: Debug

□ Enable Syslog

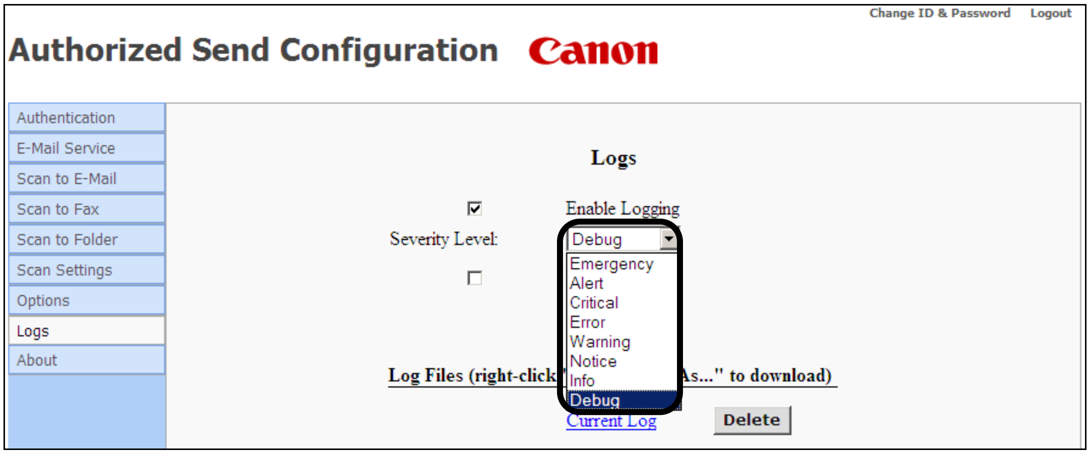
Log Files (right-click "Save Target As..." to download)

When the [Enable Logging] check box is selected, Authorized Send will log debug and error messages up to a maximum file size of 1 MB (1,024 KB).

There are can be two log files, each with a maximum file size of 512 KB.

Current Log:	Contains the most recent logging information. Once the Current Log reaches the maximum file size, it replaces the History Log (if it exists), or it creates a new History Log. The Current Log is then cleared to 0 KB.
History Log:	Contains the contents of the last Current Log that reached the maximum file size. The History Log does not exist until the Current Log reaches its maximum size and resets itself.

3. Select the severity level from the Severity Level drop-down list.



Logs

☑ Enable Logging

Severity Level: Debug

□

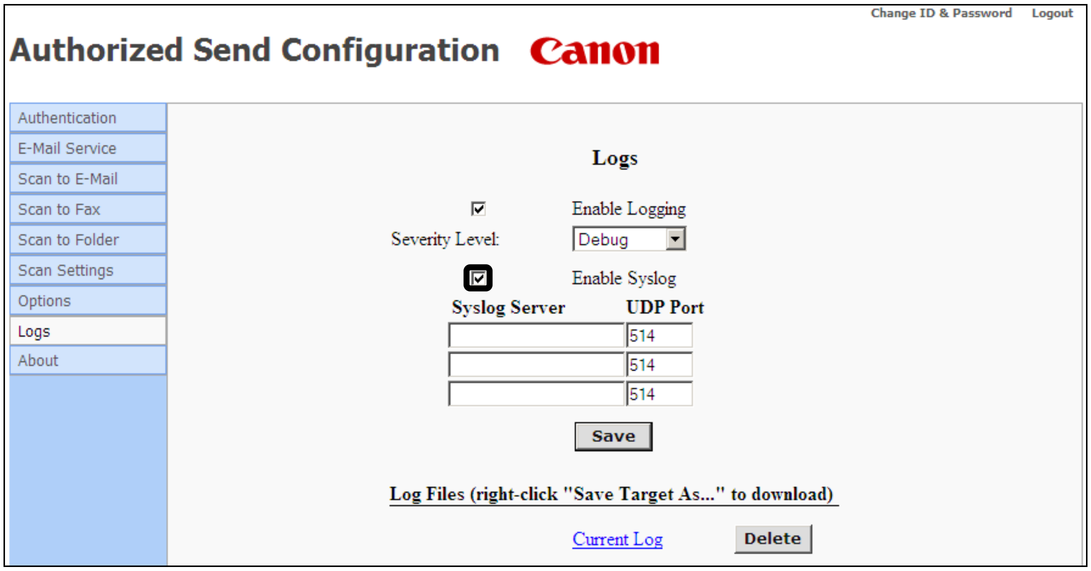
The table below shows the supported levels of increasing severity and their respective numeric codes.

Severity Level	Numeric Code
Emergency	0
Alert	1
Critical	2
Error	3
Warning	4
Notice	5
Info	6
Debug	7

When you select a severity from the drop-down list, that severity and all severities with a lower numeric value are logged.

The default setting is ‘Debug’. If [Debug] is selected, all severities are logged.

4. Select the [Enable Syslog] check box.



Logs

☑ Enable Logging

Severity Level: Debug

☑ Enable Syslog

Syslog Server	UDP Port
	514
	514
	514

If you select the [Enable Syslog] check box, at least one syslog server must be configured.

Authorized Send supports only the user-level messages (Numeric Code = 1) and security/authorization messages (Numeric Code = 4) Facilities of the Syslog RFC3164 Protocol.

User-level messages are logged locally within the Authorized Send application. Security/authorization messages are also logged locally, as well as sent to all configured remote syslog servers.

Messages are logged in the following format:
<PRI#> HEADER MSG

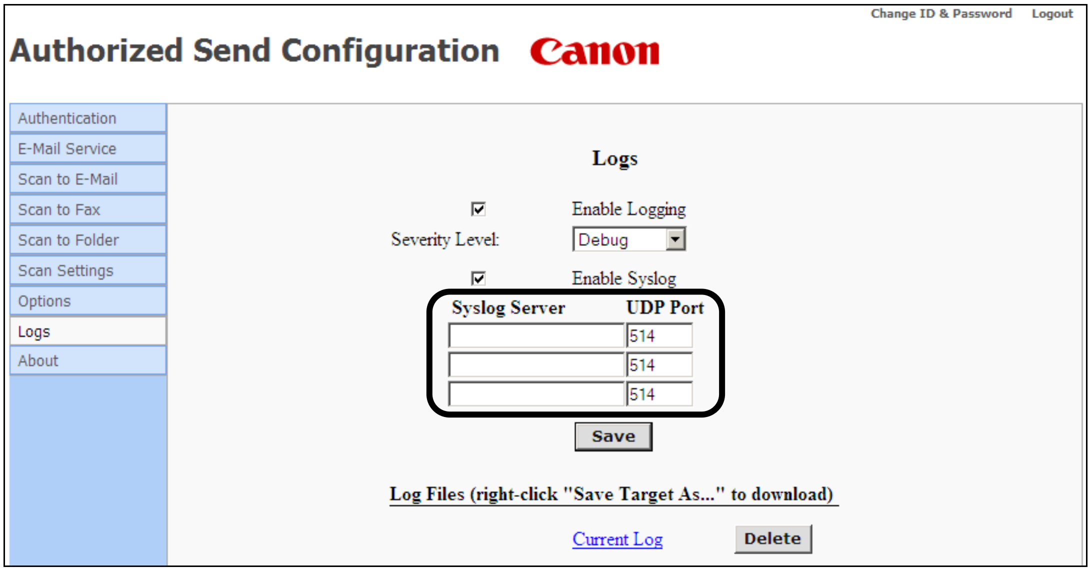
PRI = Priority number depending on the Facility and Severity.
HEADER = Mmm dd hh:mm:ss HostName/IP
MSG = Tag (the application) followed by the message.

For example: <34>Feb 23 22:14:15 iR-HostName AS sign-in failed.

NOTE

The messages sent to a remote syslog server cannot exceed 1,024 bytes. Any messages that exceed 1,024 bytes are split and sent as multiple messages.

5. Enter a syslog server's IP address under <Syslog Server> in the table ➞ enter the corresponding UDP port number for the syslog server under <UDP Port> in the table.



Logs

☑ Enable Logging

Severity Level: Debug

☑ Enable Syslog

Syslog Server	UDP Port
	514
	514
	514

Log Files (right-click "Save Target As..." to download)

You can configure up to three syslog servers. You can enter a maximum of five numbers for the UDP port.

6. Click [Save].

7. To view the log file, click [Current Log] or [History Log] (if available).

   A browser window opens to display a snapshot of the contents of the log file.

NOTE

- The log file contents displayed are not live. To view the latest contents of the log file, you must close the log window ➞ refresh the Authorized Send Configuration servlet ➞ click [Current Log] to open a new browser window.
- [History Log] only appears after the current log reaches a maximum size of 512 KB. Once the current log reaches the maximum size, it replaces the history log (if it exists), or creates a new history log.

8. To download the log file, right-click [Current Log] or [History Log] ➞ select [Save Target As] ➞ select a location to save the file.

NOTE

If HTTPS is being used for the Configuration servlet, you must first open the log file (by clicking [Current Log] or [History Log]), and then save the log file (by clicking [File] ➞ [Save As]). Right-clicking [Current Log] or [History Log] does not work with HTTPS enabled.

9. To delete the log file, click [Delete].

   If you want to disable the Log function, click the [Enable Logging] check box to clear the check mark ➞ click [Save].

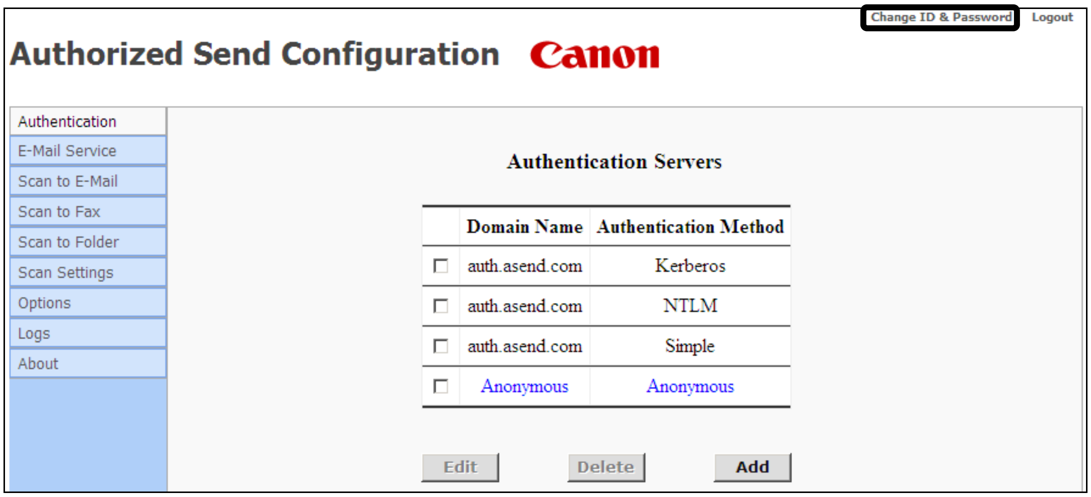
3.18 Changing the Login ID and Password

You can change your Login ID and password to log on to the Authorized Send Configuration servlet.

1. Display the Authorized Send Configuration screen and log on to the Authorized Send Configuration servlet.

   If necessary, see steps 1 and 2 of "Flow of Configuration Operations," on p. 35.

2. Click [Change ID & Password].

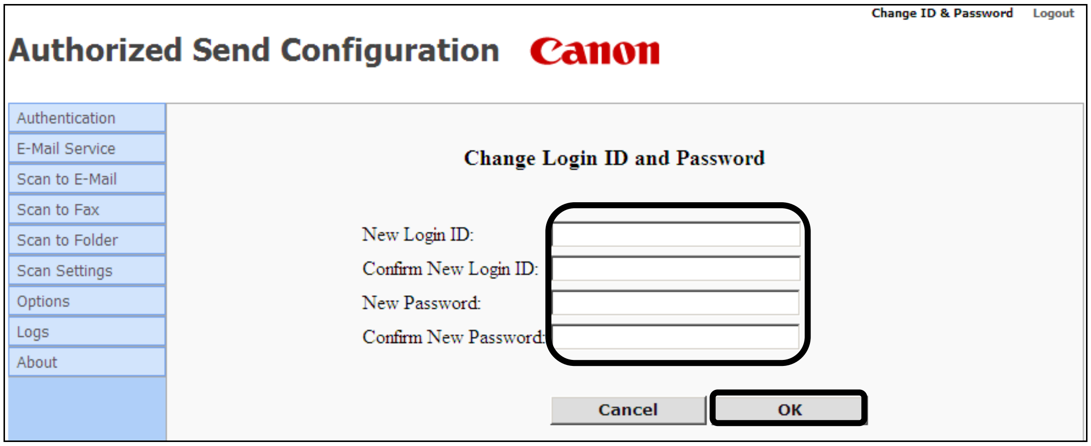


Authorized Send Configuration

Authentication Servers

	Domain Name	Authentication Method
□	auth.asend.com	Kerberos
□	auth.asend.com	NTLM
□	auth.asend.com	Simple
□	Anonymous	Anonymous

3. Enter the new login ID in the [New Login ID] text box ➞ confirm the ID in the [Confirm New Login ID] text box ➞ enter the new password in the [New Password] text box ➞ confirm the password in the [Confirm New Password] text box ➞ click [OK].



If you want to cancel changing the login ID and password, press [Cancel].

NOTE

- There is no limit to the number of characters that can be used for the new login ID and new password.
- Any alphanumeric character can be used for the new login ID and password.

3.19 Using the Brand Configuration Tool (Optional)

This section describes how to dynamically modify the appearance of the end user's interface screens using the optional Brand Configuration tool. You can customize the application's banner image and colors, portal service logo, screen colors, button colors, and special button colors.

NOTE

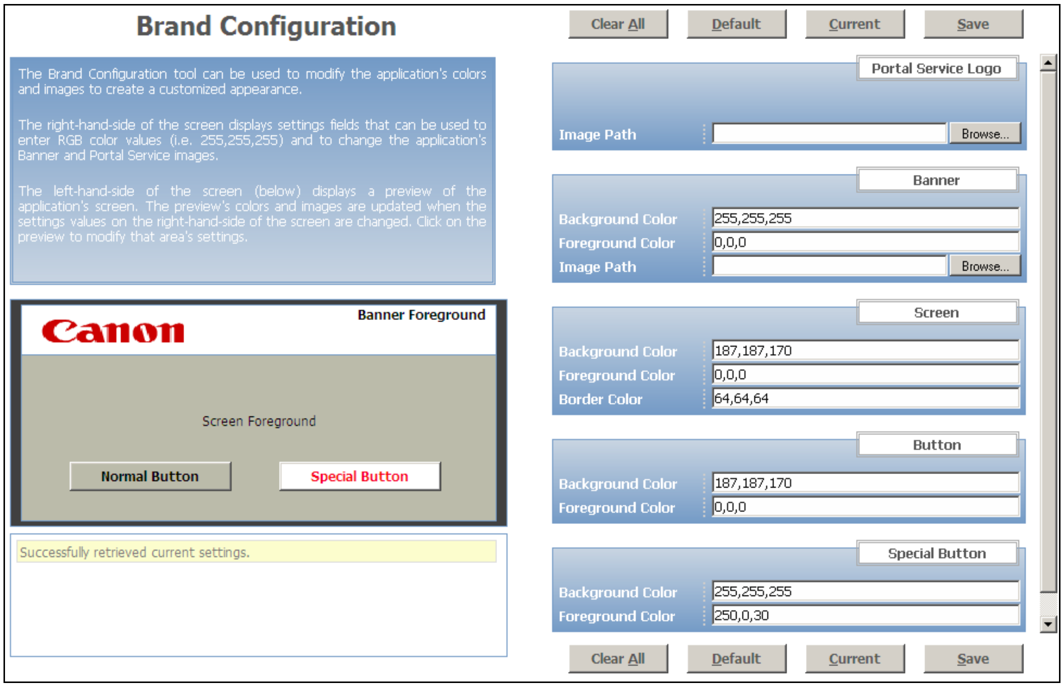
- If you are upgrading from a previous version of Authorized Send that uses the default brand configuration, the new brand configuration takes effect when Authorized Send Version 4.1 is installed.
- If you are upgrading from a previous version of Authorized Send that uses a customized brand configuration, the new brand configuration does not take effect when Authorized Send Version 4.1 is installed (the brand configuration is left as is).

1. Open a browser window ➞ enter the following URL:

   http://<device IP>:8000/AuthSendConfiguration/branding
   (Replace <device IP> with the IP address of the MEAP device.)

   IMPORTANT
   Enter **AuthSendConfiguration/branding** exactly as shown, as it is case-sensitive.

   The Brand Configuration tool screen is displayed.



Brand Configuration

The Brand Configuration tool can be used to modify the application's colors and images to create a customized appearance.

The right-hand-side of the screen displays settings fields that can be used to enter RGB color values (i.e. 255,255,255) and to change the application's Banner and Portal Service images.

The left-hand-side of the screen (below) displays a preview of the application's screen. The preview's colors and images are updated when the settings values on the right-hand-side of the screen are changed. Click on the preview to modify that area's settings.

Successfully retrieved current settings.

Portal Service Logo
Image Path:

Banner
Background Color: 255,255,255
Foreground Color: 0,0,0
Image Path:

Screen
Background Color: 187,187,170
Foreground Color: 0,0,0
Border Color: 64,64,64

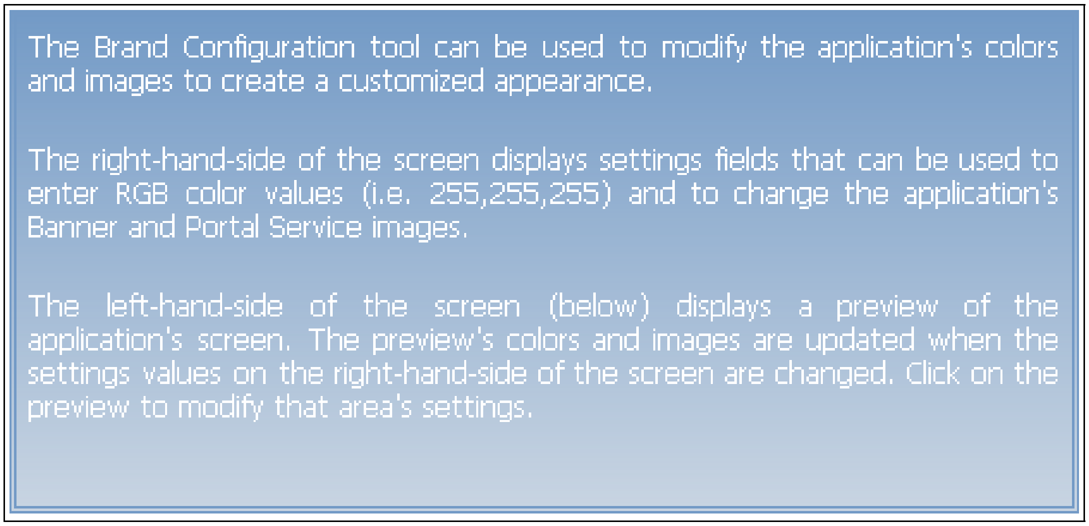
Button
Background Color: 187,187,170
Foreground Color: 0,0,0

Special Button
Background Color: 255,255,255
Foreground Color: 250,0,30

The following section describes the different areas that make up the Brand Configuration tool screen.

Description Area:

The description area displays an explanation of the Brand Configuration tool's purpose.



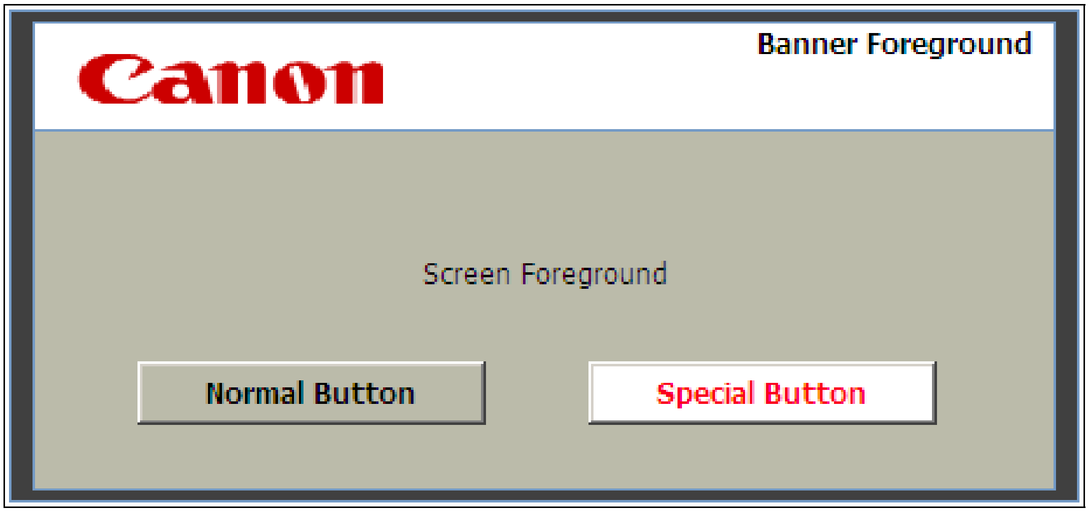
The Brand Configuration tool can be used to modify the application's colors and images to create a customized appearance.

The right-hand-side of the screen displays settings fields that can be used to enter RGB color values (i.e. 255,255,255) and to change the application's Banner and Portal Service images.

The left-hand-side of the screen (below) displays a preview of the application's screen. The preview's colors and images are updated when the settings values on the right-hand-side of the screen are changed. Click on the preview to modify that area's settings.

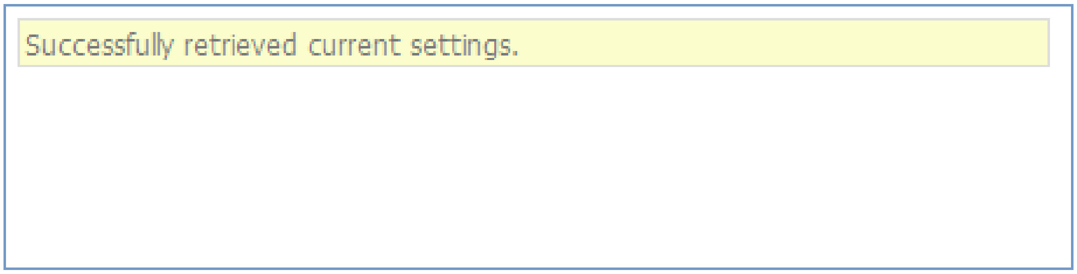
Preview Area:

The preview area displays a preview of how the end user's interface screens appear after changing the selected images and colors. This area displays a Banner Foreground, Screen Foreground, Normal Button, Special Button, and all of the images and colors relevant to each.



Status Area:

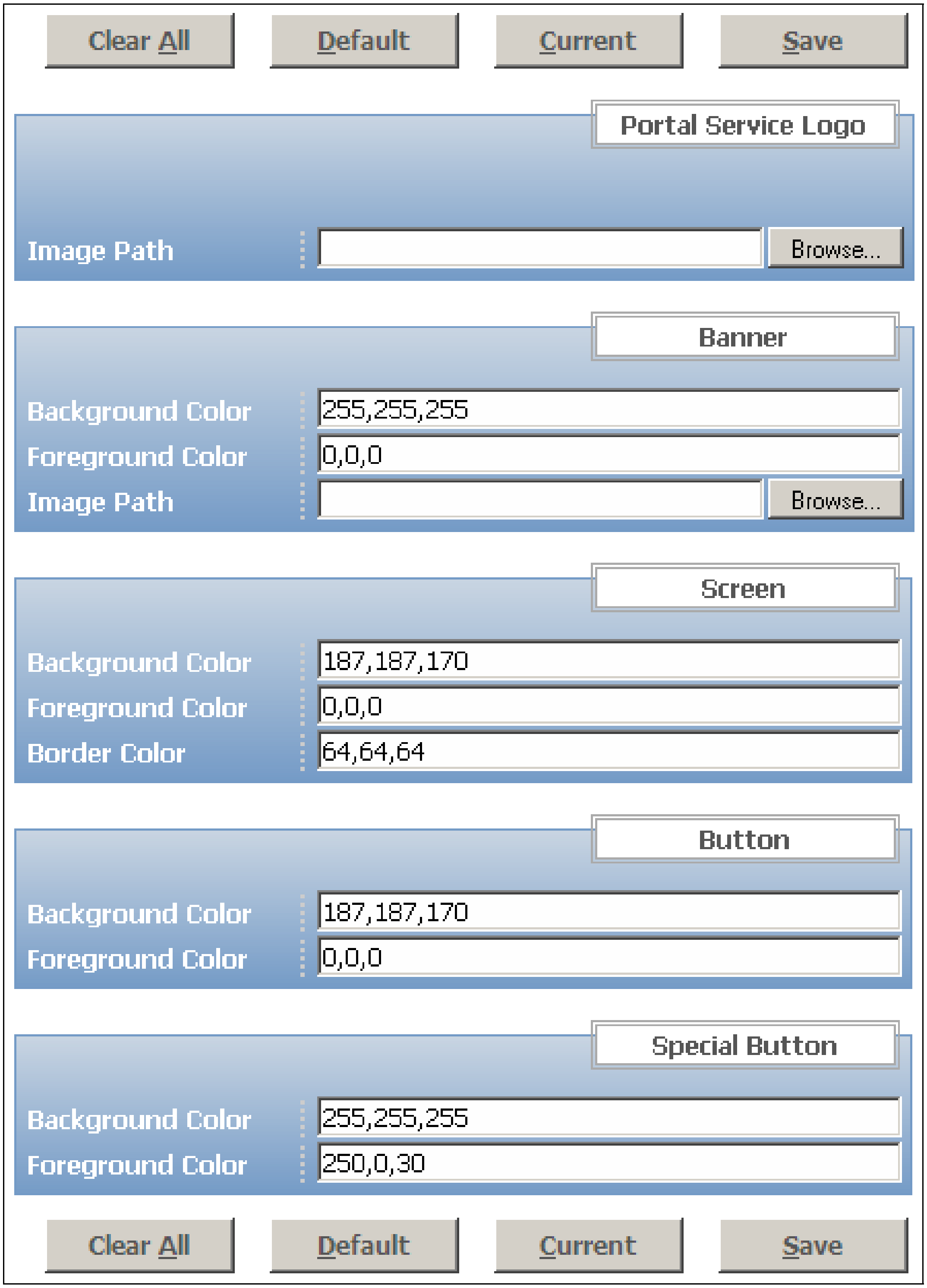
The status area displays messages as various brand configuration operations are performed. It also displays informative messages whenever errors occur. If a message is larger than the display area, a scrollbar appears to enable you to view the entire message.



Successfully retrieved current settings.

Settings Area:

The settings area displays the text boxes used for modifying image and color settings seen in the preview area. The settings area is made up of the Portal Service Logo, Banner, Screen, Button, and Special Button.



Portal Service Logo

Image Path:

Banner

Background Color: 255,255,255

Foreground Color: 0,0,0

Image Path:

Screen

Background Color: 187,187,170

Foreground Color: 0,0,0

Border Color: 64,64,64

Button

Background Color: 187,187,170

Foreground Color: 0,0,0

Special Button

Background Color: 255,255,255

Foreground Color: 250,0,30

Portal Service Logo:

The Portal Service Logo provides a text box for entering the location of the application logo you want, and provides a preview of the selected image.

Banner:

The Banner area provides text boxes for specifying the background and foreground colors, and entering the location of the banner you want.

Screen:

The Screen area provides text boxes for specifying the background, foreground, and border colors.

Button:

The Button area provides text boxes for specifying the background and foreground colors for normal buttons. A normal button is any button except for the Sign In and Sign Out buttons.

Special Button:

The Special Button area provides text boxes for specifying the background and foreground colors for special buttons. The special buttons are the Sign In and Sign Out buttons.

NOTE

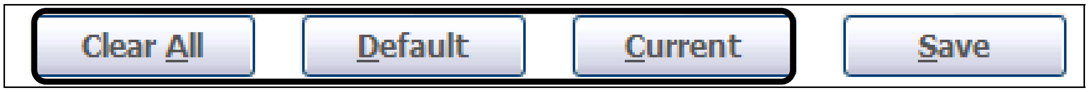
- The default values for the Portal Service Logo and Banner Image screens are:

Item	Value
Portal Service Logo	A blank image is used by default.
Banner Image	Canon

- The default values for the Background Color, Foreground Color, Border Color, Banner, Screen, Button, and Special Button screens are:

Default Color	Banner	Screen	Button	Special Button
Background Color	255, 255, 255	187, 187, 170	187, 187, 170	255, 255, 255
Foreground Color	0, 0, 0	0, 0, 0	0, 0, 0	250, 0, 30
Border Color	N/A	64, 64, 64	N/A	N/A

2. Select [Clear All], [Default], or [Current].



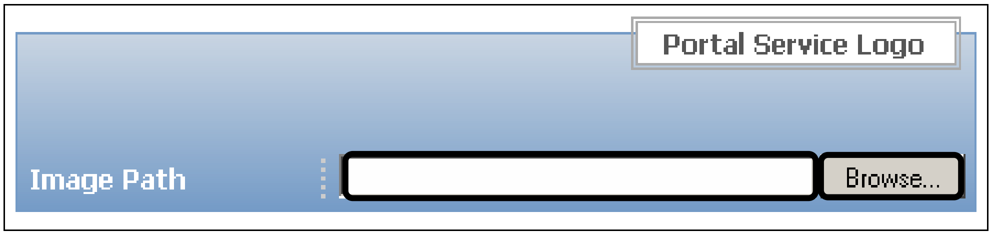
[Clear All]: Click to clear all of the settings.

[Default]: Click to load the default values for each setting and populate the corresponding text boxes in the settings area.

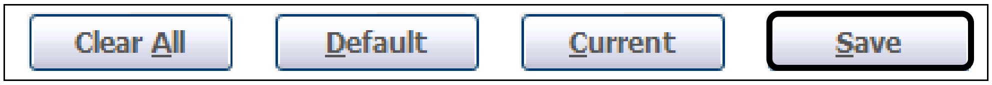
[Current]: Click to load the currently saved values for each setting and populate the corresponding text boxes in the settings area.

3. If you want to specify the end user's interface portal service logo:

3.1 Click the [Image Path] text box under <Portal Service Logo> ➞ enter the path to the image file you want to display, or click [Browse] ➞ navigate to the drive or directory containing the path to the image file you want to display.



3.2 Click [Save] to save the settings currently displayed in the settings area, and to update the end user's interface portal service logo to use the new settings.



The preview area displays the updated image.

IMPORTANT
The supported file formats are jpg, jpeg, gif, and png.

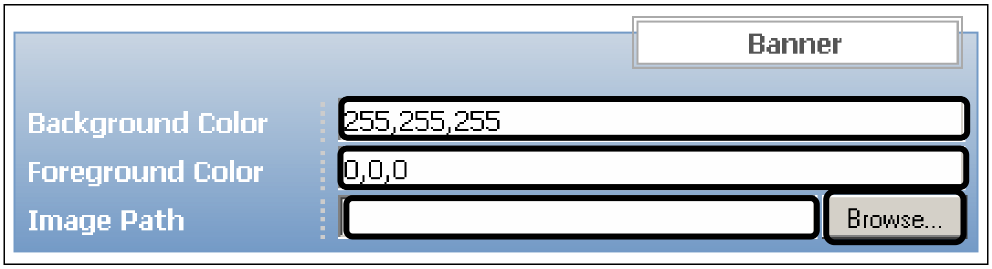
NOTE
The recommended image size is 88 pixels (W) x 23 pixels (H).

4. If you want to specify the background and foreground colors, and select the image to be displayed in the end user’s interface banner area:

   4.1 Click the [Background Color] text box under <Banner> ➞ enter three comma-separated digits representing the desired RGB color.

   4.2 Click the [Foreground Color] text box under <Banner> ➞ enter three comma-separated digits representing the desired RGB color.

   4.3 Click the [Image Path] text box under <Banner> ➞ enter the path to the image file you want to display, or click [Browse] ➞ navigate to the drive or directory containing the path to the image file you want to display.



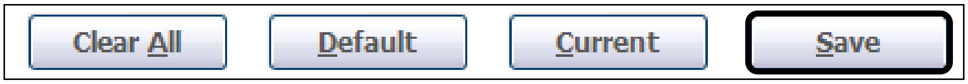
Banner

Background Color: 255,255,255

Foreground Color: 0,0,0

Image Path:

   4.4 Click [Save] to save the settings currently displayed in the settings area, and to update the end user’s interface banner to use the new settings.



The preview area displays the updated colors and image.

IMPORTANT
The supported file formats are jpg, jpeg, gif, and png.

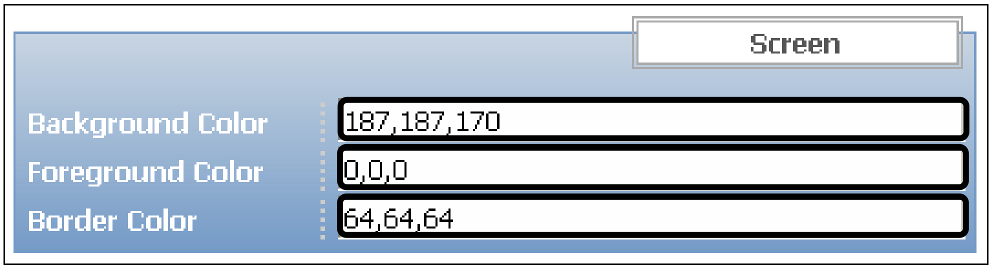
NOTE
The recommended image size is 164 pixels (W) x 43 pixels (H).

5. If you want to specify the background, foreground, and border colors to be displayed in the end user's interface screen area:

5.1 Click the [Background Color] text box under <Screen> ➞ enter three comma-separated digits representing the desired RGB color.

5.2 Click the [Foreground Color] text box under <Screen> ➞ enter three comma-separated digits representing the desired RGB color.

5.3 Click the [Border Color] text box under <Screen> ➞ enter three comma-separated digits representing the desired RGB color.



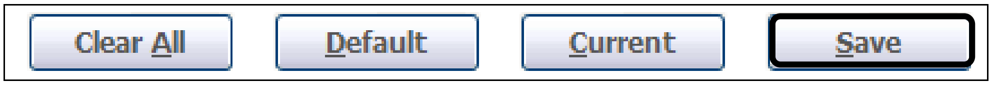
Screen

Background Color: 187,187,170

Foreground Color: 0,0,0

Border Color: 64,64,64

5.4 Click [Save] to save the settings currently displayed in the settings area, and to update the end user's interface screen to use the new settings.

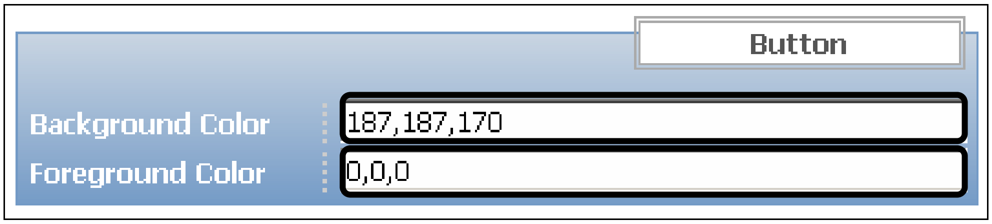


The preview area displays the updated colors.

6. If you want to specify the end user's interface background and foreground colors for the normal buttons:

   6.1 Click the [Background Color] text box under <Button> ➞ enter three comma-separated digits representing the desired RGB color.

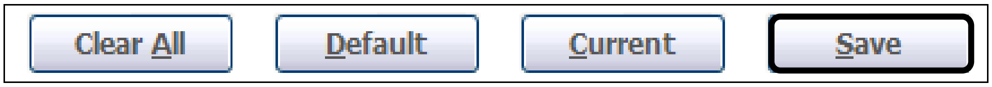
   6.2 Click the [Foreground Color] text box under <Button> ➞ enter three comma-separated digits representing the desired RGB color.



Background Color: 187,187,170

Foreground Color: 0,0,0

   6.3 Click [Save] to save the settings currently displayed in the settings area, and to update the end user's interface normal buttons to use the new settings.

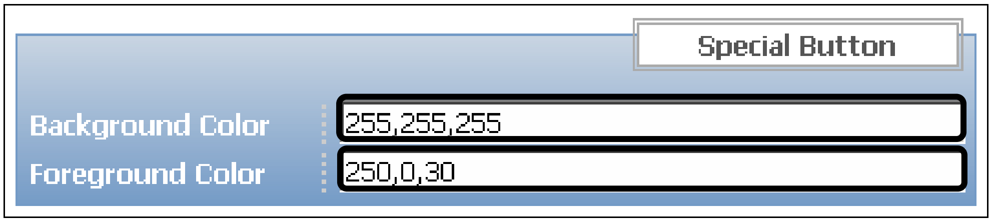


The preview area displays the updated colors.

7. If you want to specify the end user's interface background and foreground colors for the special buttons:

7.1 Click the [Background Color] text box under <Special Button> ➞ enter three comma-separated digits representing the desired RGB color.

7.2 Click the [Foreground Color] text box under <Special Button> ➞ enter three comma-separated digits representing the desired RGB color.

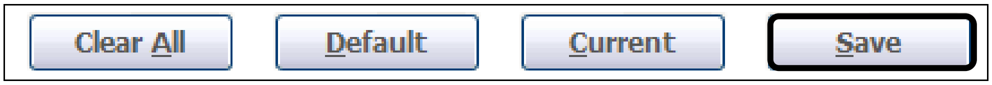


Special Button

Background Color: 255,255,255

Foreground Color: 250,0,30

7.3 Click [Save] to save the settings currently displayed in the settings area, and to update the end user's interface special buttons to use the new settings.



The preview area displays the updated colors.

This page is intentionally left blank.

Chapter 4 Configuring the MEAP Device

This chapter describes how to configure your MEAP-enabled device so that you can use it with the Authorized Send application.

✋ IMPORTANT

Inbox 99 must be available for use on the MEAP device (i.e., is not full), and with no password protection. Authorized Send temporarily stores scanned images in this inbox, and therefore, it is important that Inbox 99 have sufficient space available for these images to be stored. The images are automatically erased from Inbox 99 after scanning is complete.

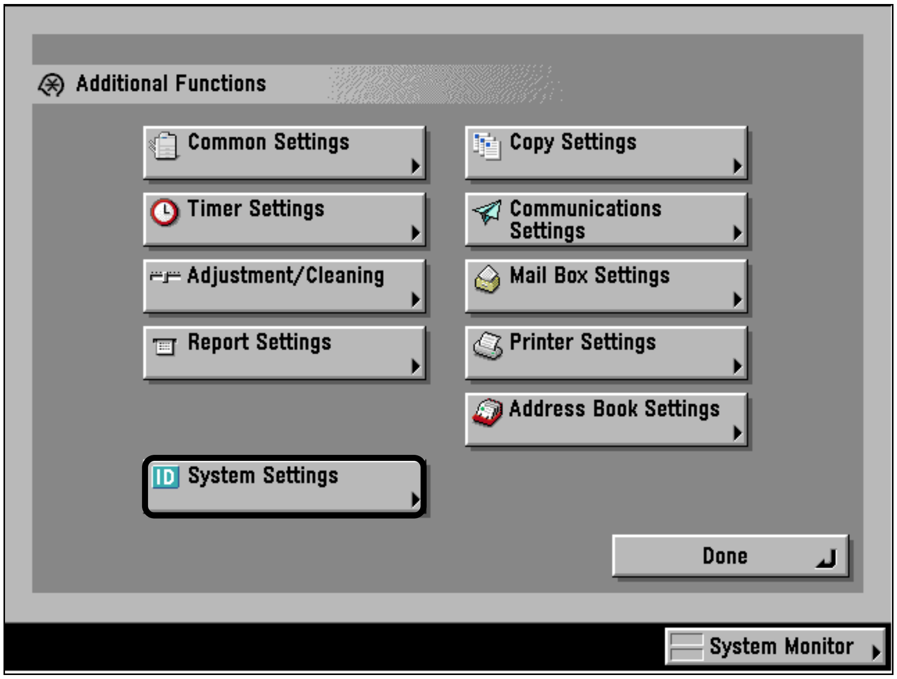
4.1 Setting DNS Server Settings

After the servers and operating environment is set up, and Authorized Send is installed and configured properly, you must configure your MEAP-enabled device.

Follow the procedure below to configure the MEAP device for Authorized Send.

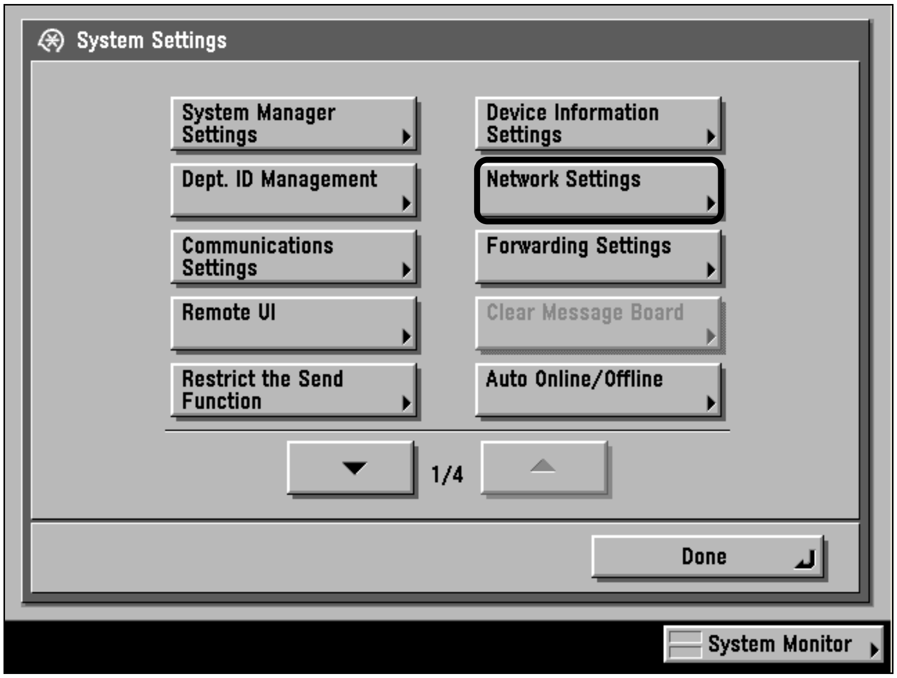
1. On the machine’s control panel, press ⊛ (Additional Functions).

2. Press [System Settings].

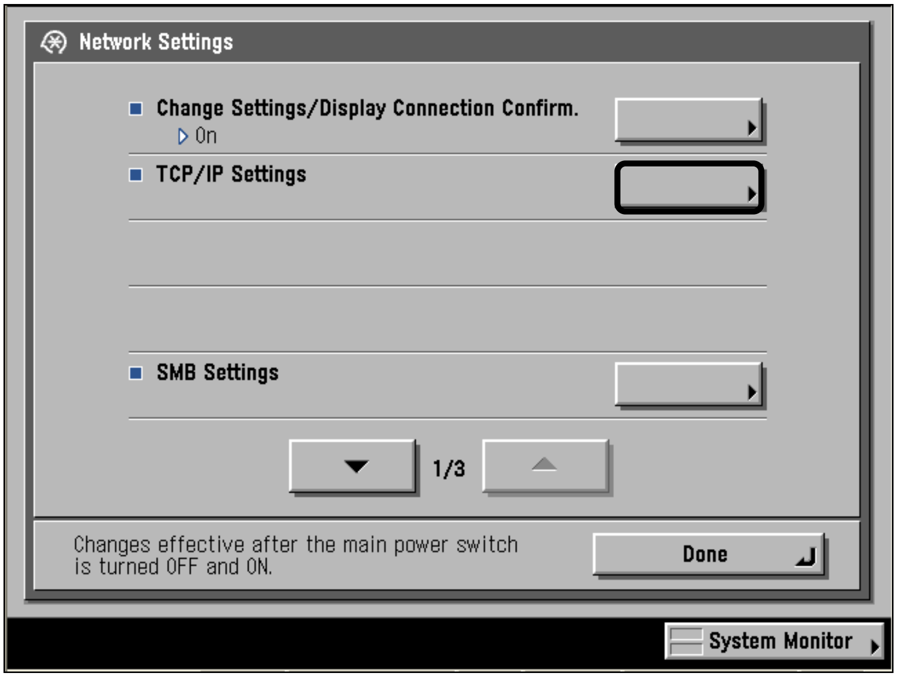


If the System Manager ID and System Password have been set, enter the System Manager ID and System Password using ⓪ – ⑨ (numeric keys) ➞ press ID (Log In/Out).

3. Press [Network Settings].

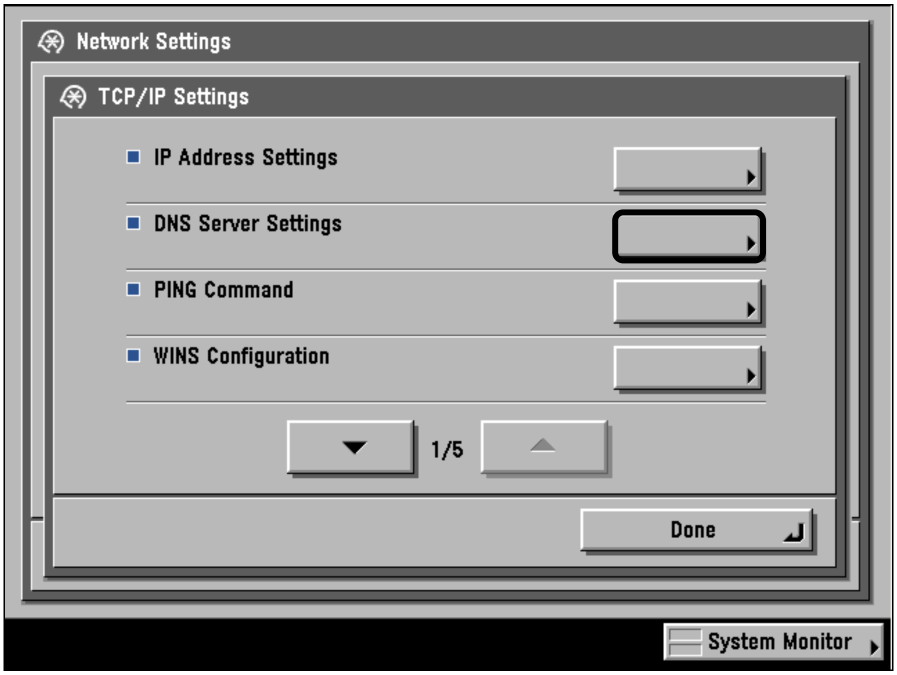


4. Press [TCP/IP Settings].

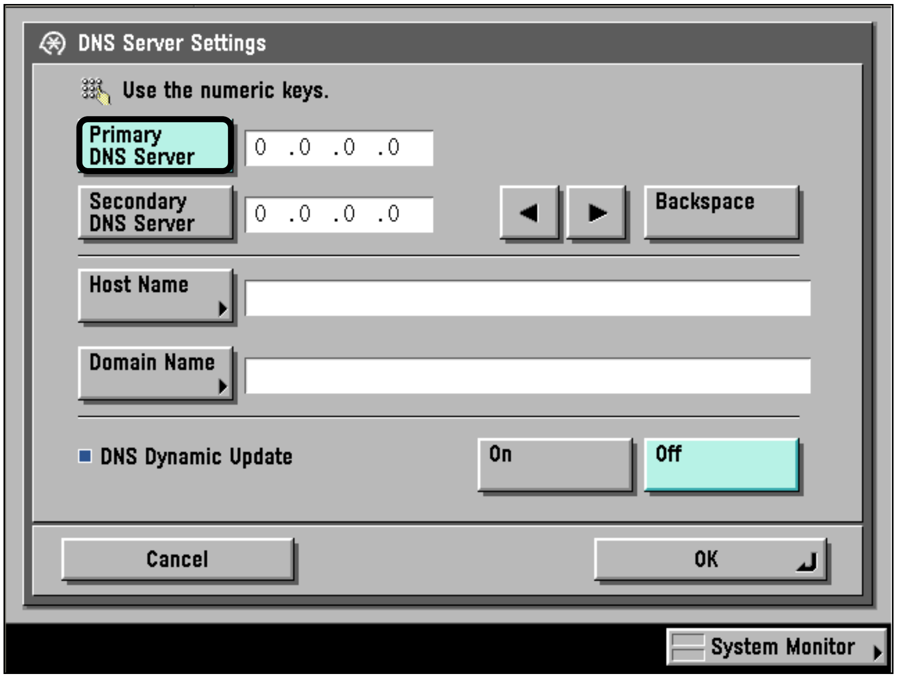


Changes effective after the main power switch is turned OFF and ON.

5. Press [DNS Server Settings].



6. Press [Primary DNS Server] ➞ enter the IP address using ⓪ – ⑨ (numeric keys).



DNS Server Settings

Use the numeric keys.

Primary DNS Server: 0 .0 .0 .0

Secondary DNS Server: 0 .0 .0 .0

Host Name:

Domain Name:

DNS Dynamic Update: On [✓ Off]

IMPORTANT

- It is not necessary to enter a [Secondary DNS Server] or [Host Name]; however, you must enter a [Domain Name].
- If you are using SMTP Authentication, make sure that the host name does not contain spaces (including trailing spaces) or trailing periods.

7. Press [Domain Name] ➞ enter the domain name ➞ press [OK].

8. Press [OK].

9. Press [Done] repeatedly until the Basic Features screen is displayed.

10. Restart the machine.

IMPORTANT

The MEAP device must be restarted before the settings can take effect.

4.2 Specifying the Auto Clear Mode for Auto Log Off

If the machine is idle for a certain period of time (after a scan to e-mail, scan to fax, or scan to folder key operation or job), you will be logged off of Authorized Send. This period of time is called the "Auto Clear Time."

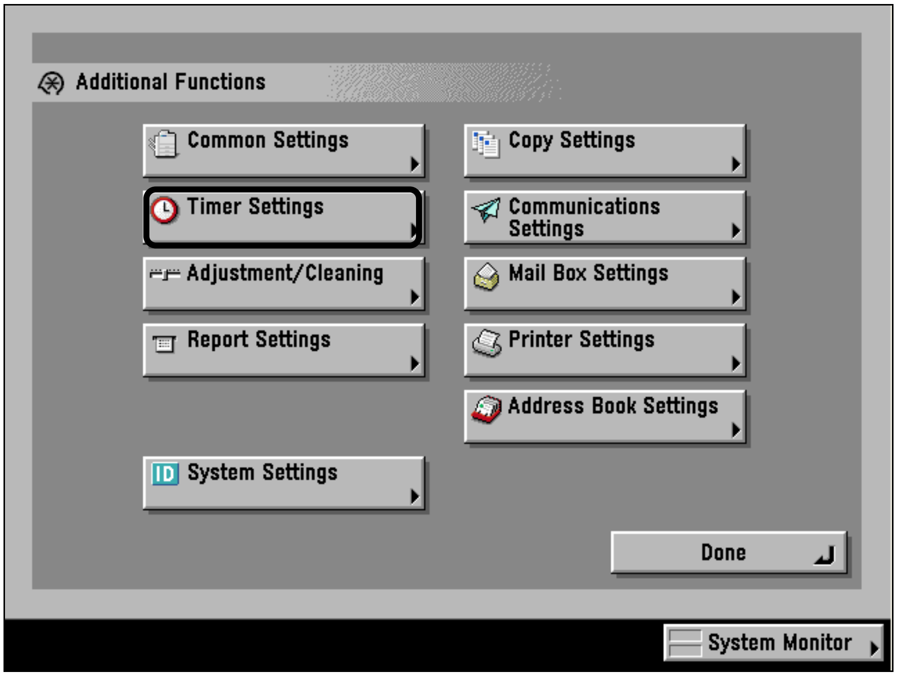
The Auto Clear Time mode can be set from ‘0’ to ‘9’ minutes in 1 minute increments, and can also be set to ‘Off’.

NOTE

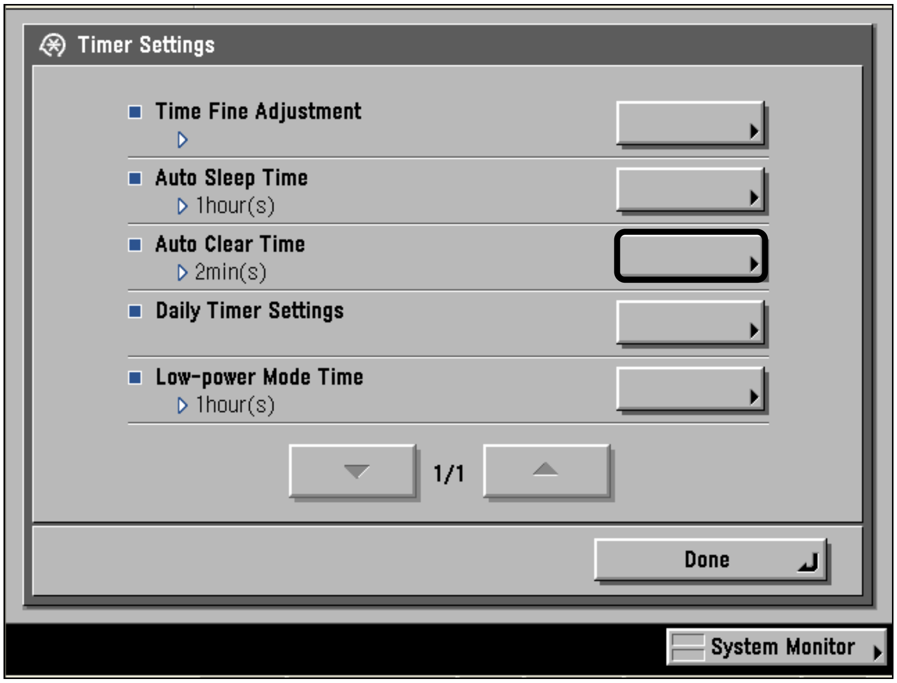
- If [0] is selected, the Auto Clear Time mode is not set.
- The default setting is ‘2’ minutes.

1. On the machine’s control panel, press ⊛ (Additional Functions).

2. Press [Timer Settings].



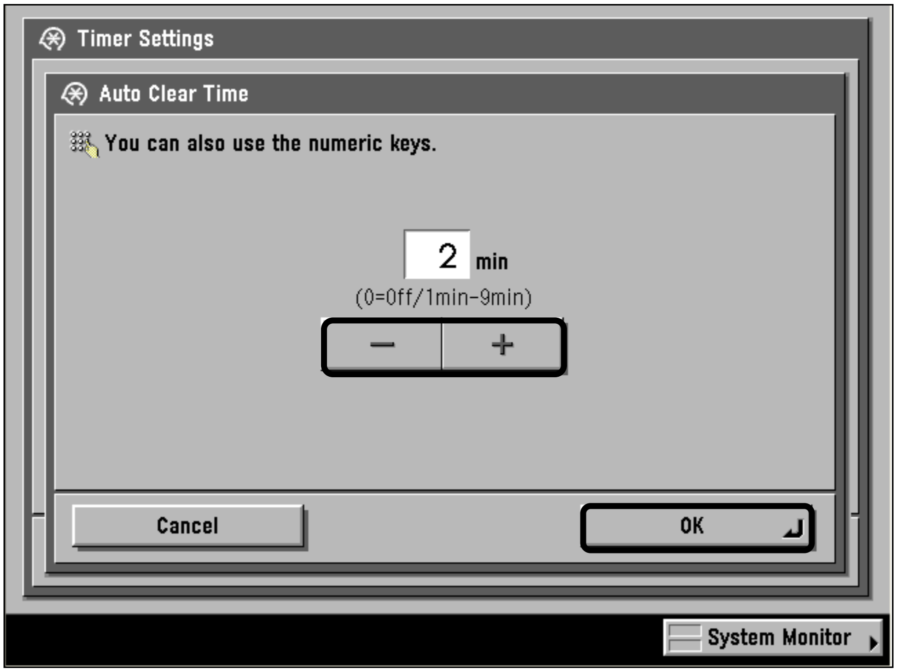
3. Press [Auto Clear Time].



Timer Settings

- Time Fine Adjustment ▷
- Auto Sleep Time ▷ 1hour(s)
- Auto Clear Time ▷ 2min(s)
- Daily Timer Settings
- Low-power Mode Time ▷ 1hour(s)

4. Press [-] or [+] to specify the desired Auto Clear Time ➞ press [OK].



Timer Settings

Auto Clear Time

You can also use the numeric keys.

2 min

(0=Off/1min-9min)

You can also enter values using ⓪ – ⑨ (numeric keys).

5. Press [Done] repeatedly until the Basic Features screen is displayed.

4.3 Synchronizing the Device and Server Time

If you configure an authentication server or address book server for Kerberos authentication, you must ensure that the device clock and server clock are synchronized within the maximum server specified clock skew tolerance of ‘5’ minutes. When you authenticate using Kerberos, if there is more than a 5 minute time difference between the device clock and server clock, an error message is displayed.

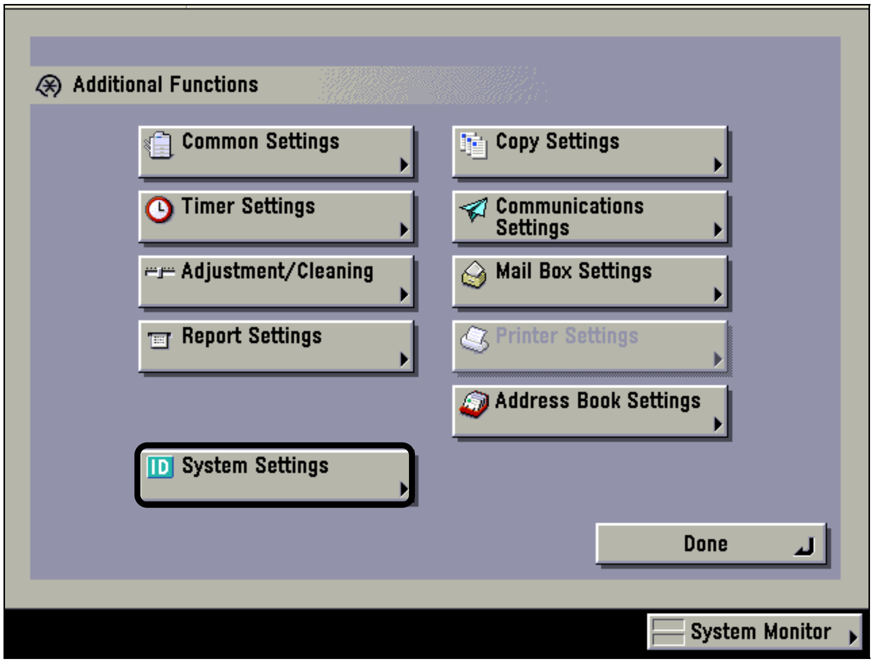
You can manually adjust the device time to synchronize with the server time, or you can set to automatically synchronize the device clock with the server clock.

4.3.1 Specifying Automatic Time Synchronization

You can set the SNTP (Simple Network Time Protocol) settings to enable the device to automatically synchronize its system time with a public time server.

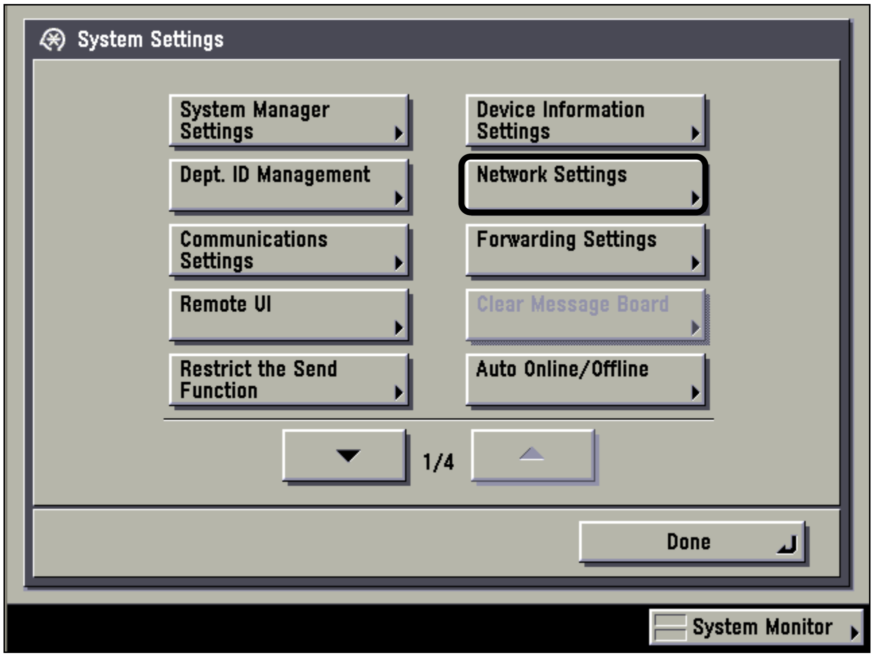
1. On the machine’s control panel, press ⊛ (Additional Functions).

2. Press [System Settings].

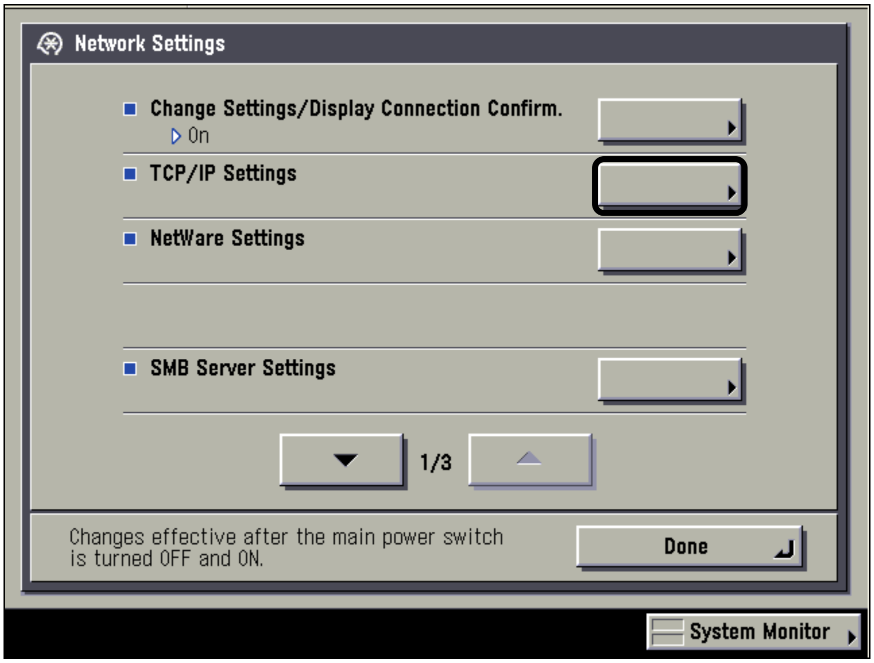


If the System Manager ID and System Password have been set, enter the System Manager ID and System Password using ⓪ – ⑨ (numeric keys) ➞ press 🆔 (Log In/Out).

3. Press [Network Settings].



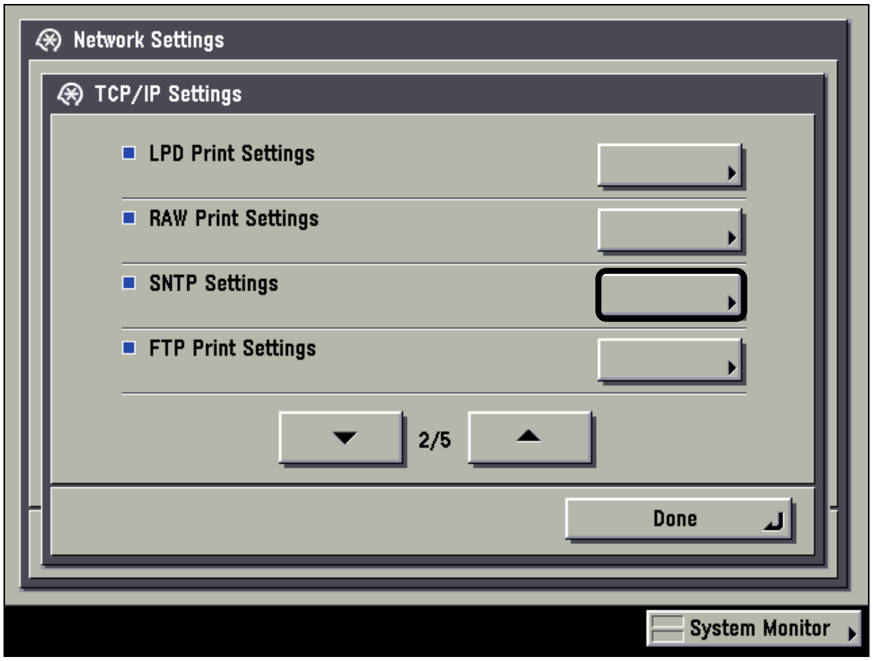
4. Press [TCP/IP Settings].



Change Settings/Display Connection Confirm.
On

Changes effective after the main power switch is turned OFF and ON.

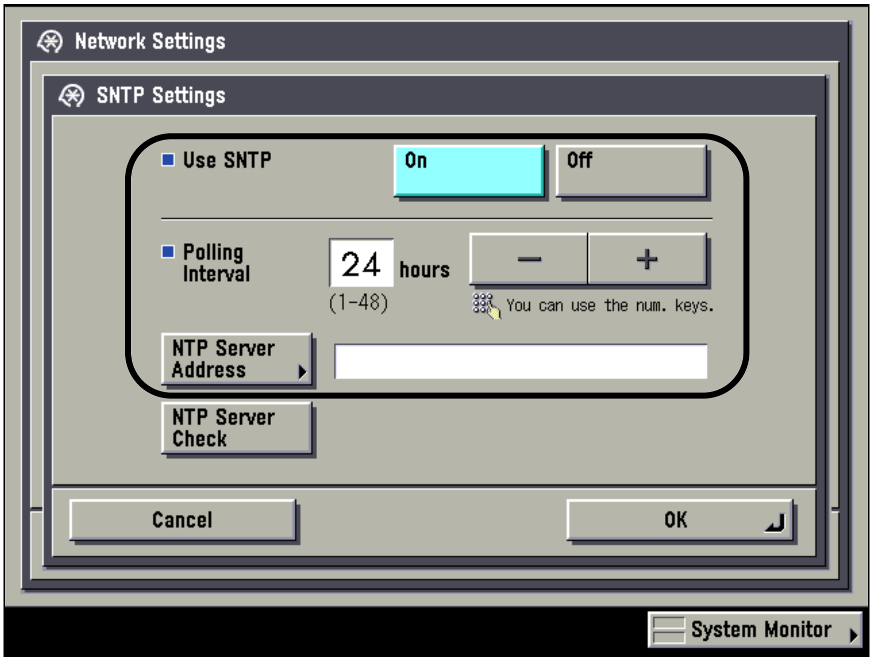
5. Press [SNTP Settings].



NOTE

If the desired setting is not displayed, press [▼] or [▲] to scroll to the desired setting.

6. Specify the SNTP settings.



Network Settings

SNTP Settings

Use SNTP: On

Polling Interval: 24 hours (1-48)

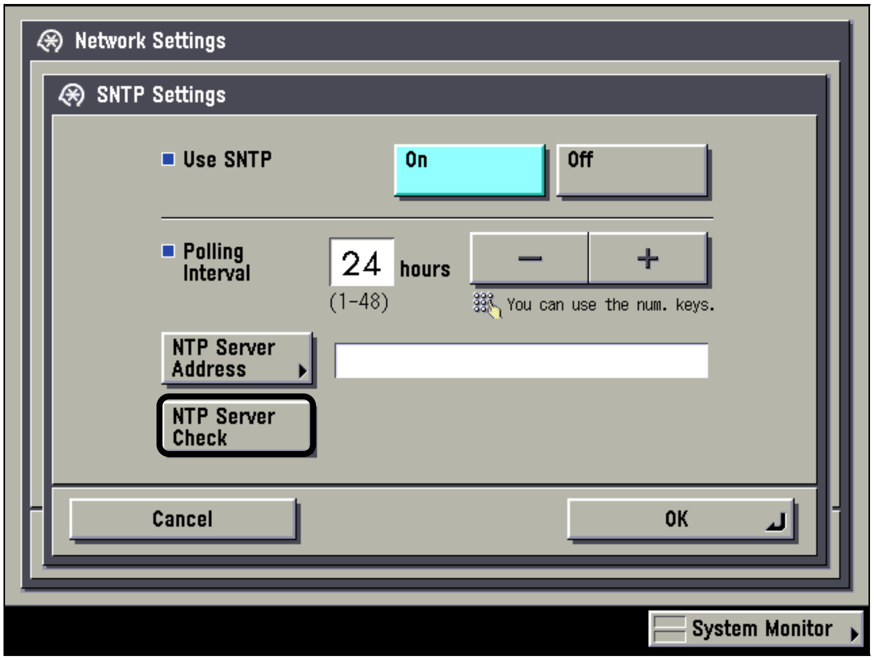
You can use the num. keys.

<Use SNTP>: Select [On] to perform time synchronization using SNTP.

<Polling Interval>: Select the interval for performing time synchronization from ‘1’ to ‘48’ hours.

[NTP Server Address]: Enter the NTP server address or host name.

7. Press [NTP Server Check] to check the status of the NTP server.



If <OK> is displayed next to [NTP Server Check], time synchronization is working correctly via SNTP.

If <Error> is displayed next to [NTP Server Check], check the settings for [NTP Server Address] set in step 6.

8. Press [OK].

IMPORTANT

To perform time synchronization via SNTP, it is necessary to set the time zone of the region in which you are using the machine in advance. For instructions on how to set the time zone, see the *Reference Guide* that came with your machine.

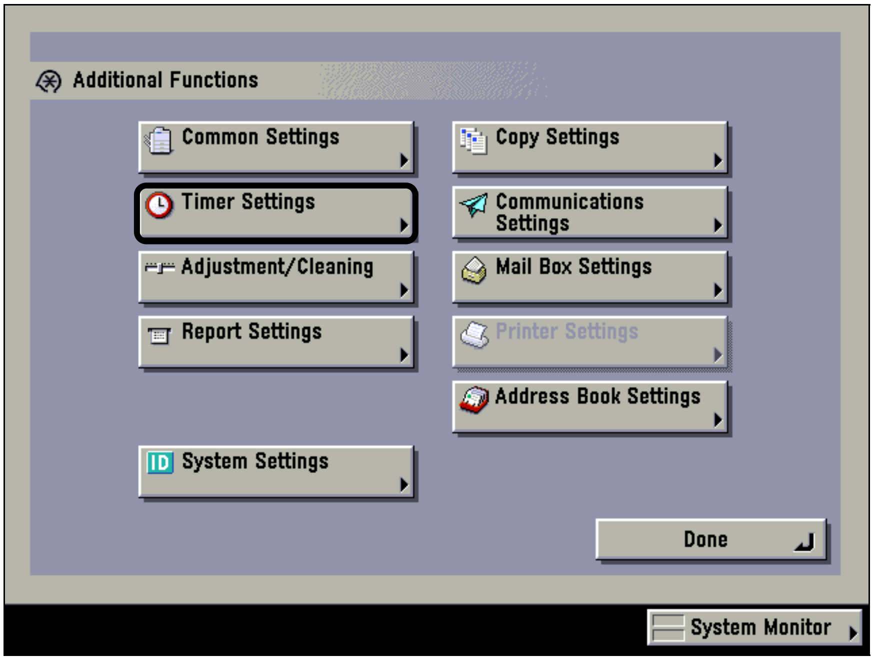
9. Press [Done] repeatedly until the Basic Features screen is displayed.

4.3.2 Manually Adjusting the Device Time

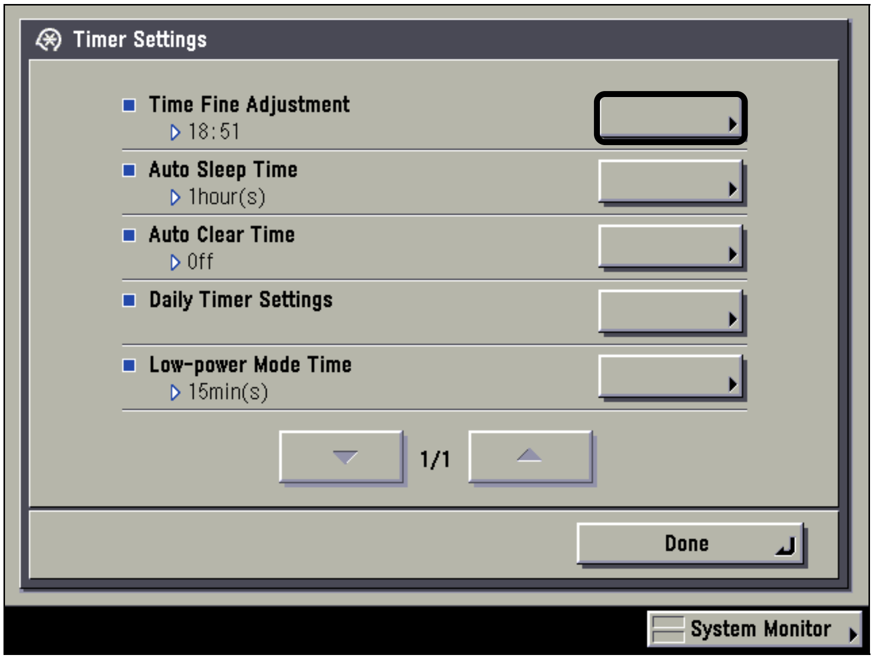
You can manually adjust the device time to match the Kerberos authentication server or address book server time.

1. On the machine’s control panel, press ⊛ (Additional Functions).

2. Press [Timer Settings].

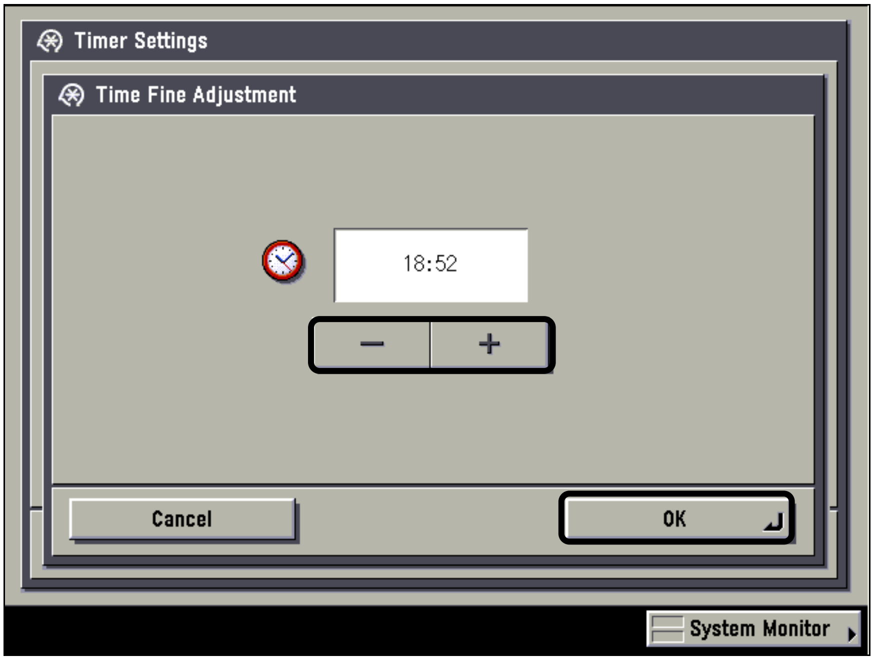


3. Press [Time Fine Adjustment].


Timer Settings

- Time Fine Adjustment
  ▷ 18:51
- Auto Sleep Time
  ▷ 1hour(s)
- Auto Clear Time
  ▷ Off
- Daily Timer Settings
- Low-power Mode Time
  ▷ 15min(s)

4. Press [-] or [+] to adjust the time as necessary → press [OK].


Timer Settings

Time Fine Adjustment

18:52

5. Press [Done] repeatedly until the Basic Features screen is displayed.

Chapter 5 Troubleshooting

This chapter explains the various issues that may arise when installing and configuring the necessary components of the Authorized Send application, along with possible causes and remedies.

Problem You cannot connect to the network.

Remedy Make sure that:

- The IP addresses of the MEAP device and server PCs are correct, and that you can ping the device.
- The server PC is on the network.
- You are not using a proxy server.

Problem The Authorized Send application is not functioning properly.

Remedy Verify that the supported MEAP contents and system software versions are installed on the MEAP device.

Problem When creating a share name on the Authorized Send Configuration screen, the message <Connection failed. Could not resolve host name: xxx.> is displayed.

Remedy Make sure that the MEAP device is on the same domain as your domain controller. (See "Setting DNS Server Settings," on p. 135.)

Problem Cannot access SMS.

Remedy Two people cannot be logged on to SMS at the same time. Make sure that you are the only one logged on to SMS, and that you have the correct IP address and port number (:8000).

Problem The Authorized Send application cannot be installed or started.

Remedy Check to make sure that:

- Another application is not using resources.
- An authorized copy of the software is being used.

Problem The [Scan to E-Mail] button is disabled.

Remedy Check to make sure that:

- An e-mail address is specified in the user's address book account.
- An SMTP server address is configured for Authorized Send.
- For more information, see "LDAP Failure Notification Messages," on p. 168.

IMPORTANT
It is necessary for the user to log off, and then log back on after the changes mentioned above have been made to activate the [Scan to E-Mail] key.

Problem The Browse feature in the Scan to Folder function only displays non-hidden and non-system shares (i.e., the first level directory under the root is not displayed in the Browse window).

Remedy Specify the first level directory share in the path text box, and then you can browse from this directory.

Problem The address book feature in the Scan to E-Mail function does not work.

Remedy Make sure that the correct Base DN (Distinguished Name) is entered in the [E-Mail Service] ➞ [Address Book] tab in the Authorized Send Configuration servlet. (See "Creating an Address Book Server," on p. 67.)

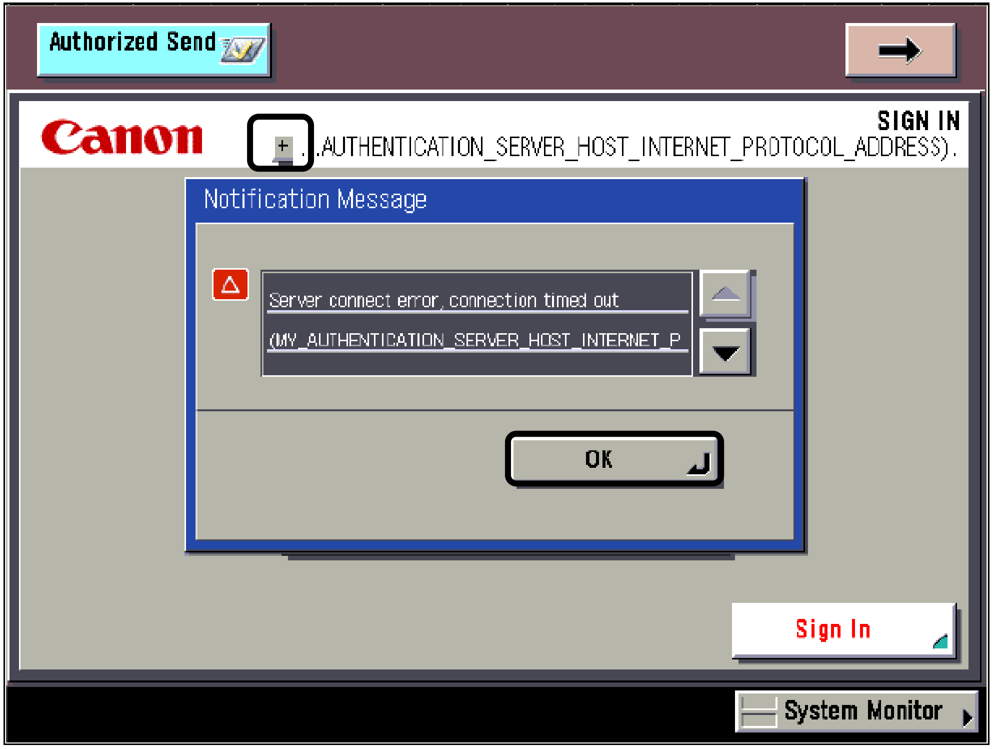
Chapter 6 List of Error Messages

This chapter explains the various messages that appear on the Authorized Send Configuration servlet screen or on the touch panel display of the MEAP device, along with possible causes and remedies.

Any words that appear italicized are variables, and will be replaced with their corresponding values on the actual application screen.

NOTE

- If an error message is too long to display in full in the Message Notification Section on the touch panel display, click [+] next to the message to display a pop-up dialog box containing the full text of the error message ➞ click [OK] to close the dialog box.



+ ..AUTHENTICATION_SERVER_HOST_INTERNET_PROTOCOL_ADDRESS).

Server connect error, connection timed out
(MY_AUTHENTICATION_SERVER_HOST_INTERNET_P

- If any error messages are displayed but are not listed in this chapter, contact your local authorized Canon dealer.

6.1 Configuration Screen Error Messages

Configuration screen messages are displayed on the Configuration screen of the Authorized Send Configuration servlet. If an error occurs during the configuration process, it is displayed in the body of the Configuration servlet screen, and is listed here.

6.1.1 Authentication Servers Screen Error Message

This section explains the Authentication Servers screen error message, along with a possible cause and remedy. For more information on the remedy, see “Creating an Authentication Server,” on p. 49.

Message	Cause	Remedy
Maximum authentication servers have been created. To create a new authentication server, you have to delete the old one(s) first.	The maximum number of 10 authentication servers has been created.	Delete the old authentication server(s) first, and make sure you do not exceed 10 servers in total.

6.1.2 Create/Update Authentication Server Screen Error Messages

This section explains the Create Authentication Server and Update Authentication Server screen error messages, along with possible causes and remedies. For more information on the remedies, see “Creating an Authentication Server,” on p. 49, and “Editing an Authentication Server,” on p. 62.

Message	Cause	Remedy
Authentication Host is missing.	The [Host] text box is blank.	Enter the DNS name or IP address of the authentication server.
Authentication Port is missing.	The [Port] text box is blank.	Enter the numeric value for the connecting port number of the authentication server.
Authentication Port has to be a number.	A non-numeric value is entered in the [Port] text box.	Enter the numeric value for the connecting port number of the authentication server.
Authentication Port cannot be zero.	Zero is entered in the [Port] text box.	Enter the numeric value greater than zero for the connecting port number of the authentication server.

Message	Cause	Remedy
Authentication Port has to be a positive number.	A negative number is entered in the [Port] text box.	Enter the numeric value greater than zero for the connecting port number of the authentication server.
Authentication Hostname is missing.	The [Hostname] text box is blank.	Enter the host name of the authentication server.
Authentication Public DN is missing.	The [Public DN] text box is blank.	Enter the public DN.
Authentication LDAP Match Attribute is missing.	The [LDAP Match Attribute] text box is blank.	Enter the LDAP match attribute.
Authentication Search Root is missing.	The [Search Root] text box is blank.	Enter the search root.
Anonymous User Name is missing.	The [Anonymous User Name] text box is blank.	Enter the anonymous user name for anonymous sending.
Anonymous User Name is too long. It cannot exceed 40 characters.	The anonymous user name in the [Anonymous User Name] text box exceeds 40 characters.	Make sure the anonymous user name does not exceed 40 characters.
Anonymous User Name cannot contain the following symbols: '*x*', '*y*', '*z*'…	The [Anonymous User Name] text box contains '*x*', '*y*', and '*z*' which represent invalid symbols, such as '\', ':', '?', etc.	Make sure the anonymous user name is using valid symbols.
Anonymous User E-Mail is not valid.	An e-mail address with an invalid format is entered in the [Anonymous User E-Mail] text box.	Make sure the e-mail address format is valid. See step 5.4 in "Creating an Authentication Server," on p. 49.
Anonymous User E-Mail is not valid: local part cannot be empty	The part before the '@' symbol is blank.	Make sure the part before the '@' symbol is not blank.
Anonymous User E-Mail is not valid: local part cannot exceed 64 characters	The part before the '@' symbol exceeds 64 characters.	Make sure the part before the '@' symbol does not exceed 64 characters.
Anonymous User E-Mail is not valid: dot, '.', cannot be the first or the last character in the local part	The dot, '.', is the first or last character in the local part.	Make sure the dot, '.', is not the first or last character in the local part.
Anonymous User E-Mail is not valid: *'non-ASCII printable character'* is not an ASCII printable character.	A non-ASCII printable character is entered.	Make sure an ASCII printable character is entered.
Anonymous User E-Mail is not valid: dot, '.', cannot appear consecutively in the local part.	The dot, '.', is entered consecutively in the local part.	Make sure the dot, '.', is not entered consecutively in the local part.

Message	Cause	Remedy
Anonymous User E-Mail is not valid: local part cannot contain character(s) ‘?’, ‘&’	The local part contains non-alphanumeric values other than ‘.’, ‘-’, and ‘_’ (such as ‘?’, ‘&’, ‘$’, ‘#’, ‘%’, etc.).	Make sure the local part contains only the non-alphanumeric values ‘.’, ‘-’, and ‘_’.
Anonymous User E-Mail is not valid: domain cannot be empty if ‘@’ is present.	The symbol, ‘@’, is present, but the domain part is blank.	Make sure if the symbol, ‘@’, is present, the domain part is not blank.
Anonymous User E-Mail is not valid: domain cannot exceed 255 characters.	The domain part exceeds 255 characters.	Make sure the domain part does not exceed 255 characters.
Anonymous User E-Mail is not valid: hyphen, ‘-’, or dot, ‘.’, cannot be the first or the last character in the domain.	The hyphen, ‘-’, or dot, ‘.’, appear first or last in the domain.	Make sure the hyphen, ‘-’, or dot, ‘.’, does not appear first or last in the domain.
Anonymous User E-Mail is not valid: hyphen, ‘-’, or dot, ‘.’, cannot appear consecutively in the domain.	The hyphen, ‘-’, or dot, ‘.’, appears consecutively in the domain.	Make sure the hyphen, ‘-’, or dot, ‘.’, does not appear consecutively in the domain.
Anonymous User E-Mail is not valid: domain cannot contain character(s) ‘?’, ‘&’	The domain contains non-alphanumeric values other than ‘.’, ‘-’, and ‘_’ (such as ‘?’, ‘&’, ‘$’, ‘#’, ‘%’, etc.).	Make sure the domain contains only the non-alphanumeric values ‘.’, ‘-’, and ‘_’.
Domain name is missing.	The [Domain Name] text box is blank.	Enter the domain name of the authentication server.
Pre-Set Share Search Root cannot be empty.	The [Search Root] text box for the Retrieve Home Directory function is blank.	Enter the search root.
NTLM domain name cannot be empty.	The [NTLM domain name] text box is blank.	Enter the NTLM domain name.
Cannot pull a live domain controller from DNS servers.	The [Pull host from DNS] radio button is set to ‘Yes’ and a live domain controller cannot be found.	Check the configuration and try again.
Connection Failed. Could not connect to *x:y*	The connection to the authentication server failed because Authorized Send cannot connect to the host name, represented by *x*, and the port, represented by *y*.	Check the host name and/or port and try again.
Connection Failed. Could not resolve host name: *x*.	The connection to the authentication server failed because Authorized Send cannot resolve the host name, represented by *x*.	Check the host name and/or server configuration and try again.

Message	Cause	Remedy
Duplicated authentication server: an authentication server with domain [*x*] and authentication method [*y*] already exists.	An authentication server already exists where the domain is represented by *x*, and the authentication method is represented by *y*.	Check the authentication server, domain, and authentication method and try again.

6.1.3 E-Mail Service Configuration Screen Error Messages

This section explains the E-mail Service Configuration screen error messages, along with possible causes and remedies. For more information on the remedies, see “Configuring the E-Mail Service Settings,” on p. 65.

Message	Cause	Remedy
SMTP Server Address is missing.	The [SMTP Server Address] text box is blank.	Enter the SMTP server address.
SMTP Server Port has to be a number.	A non-numeric value is entered in the [Port] text box, or the [Port] text box is blank.	Enter the numeric value for the connecting port number of the SMTP server.
SMTP Server Port cannot be zero.	Zero is entered in the [Port] text box.	Enter the numeric value greater than zero for the connecting port number of the SMTP server.
SMTP Server Port has to be a positive number.	A negative number is entered in the [Port] text box.	Enter the numeric value greater than zero for the connecting port number of the SMTP server.
SMTP Public Username Missing.	The [SMTP Public Username] text box is blank.	Enter the SMTP public username.
SMTP Public Password Missing.	The [SMTP Public Password] text box is blank.	Enter the SMTP public password.
Connection Failed. Could not connect to *x*:*y*	The connection to the SMTP server failed because Authorized Send cannot connect to the host name, represented by *x*, and the port, represented by *y*.	Check the host name and/or port and try again.
Connection Failed. Could not resolve host name: *x*.	The connection to the SMTP server failed because Authorized Send cannot resolve the host name, represented by *x*.	Check the host name and/or server configuration and try again.

6.1.4 Address Book Servers Screen Error Message

This section explains the Address Book Servers screen error message, along with a possible cause and remedy. For more information on the remedy, see "Creating an Address Book Server," on p. 67.

Message	Cause	Remedy
Maximum address book servers have been created. To create a new address book server, you have to delete the old one(s) first.	The maximum number of 10 address book servers has been created.	Delete the old address book server(s) first, and make sure you do not exceed 10 servers in total.

6.1.5 Create/Update Address Book Server Screen Error Messages

This section explains the Create Address Book Server and Update Address Book Server screen error messages, along with possible causes and remedies. For more information on the remedies, see "Creating an Address Book Server," on p. 67, and "Editing an Address Book Server," on p. 90.

Message	Cause	Remedy
Address Book Port has to be a number.	A non-numeric value is entered in the [Port] text box.	Enter a numeric value for the port.
Address Book Port cannot be zero.	Zero is entered in the [Port] text box.	Enter a numeric value greater than zero for the port.
Address Book port has to be a positive number.	A negative number is entered in the [Port] text box.	Enter a numeric value greater than zero for the port.
Cannot pull a live domain controller from DNS servers.	The [Pull Host from DNS] radio button is set to 'Yes' and a live domain controller cannot be found.	Check the configuration and try again.
Address Book Host is missing.	The [Host] text box is blank.	Enter the DNS name or IP address of the address book server.
Address Book Port is missing.	The [Port] text box is blank.	Enter a valid number for the port.
Address Book Hostname is missing.	The [Hostname] text box is blank.	Enter the host name of the address book server.
Address Book Public DN is missing.	The [Public DN] text box is blank.	Enter the public DN.
Address Book Public User Name is missing.	The [Public User Name] text box is blank.	Enter the public user name.

Message	Cause	Remedy
Address Book Domain is missing.	The [Domain Name] text box is blank.	Enter the domain name of the address book server.
Address Book Search Root is missing.	The [Search Root] text box is blank.	Enter the search root.
Address Book LDAP Match Attribute is missing.	The [LDAP Match Attribute] text box is blank.	Enter the LDAP match attribute.
Address Book LDAP Email Attribute is missing.	The [LDAP Email Attribute] text box is blank.	Enter the LDAP e-mail attribute.
Connection Failed. Could not connect to *x*:*y*	The connection to the address book server failed because Authorized Send cannot connect to the host name, represented by *x*, and the port, represented by *y*.	Check the host name and/or port and try again.
Connection Failed. Could not resolve host name: *x*.	The connection to the address book server failed because Authorized Send cannot resolve the host name, represented by *x*.	Check the host name and/or server configuration and try again.
Duplicated address book server: an address book server with domain [*x*] and bind method [*y*] already exists.	An address book server already exists where the domain is represented by *x*, and the bind method is represented by *y*.	Check the address book server, domain, and bind method and try again.

6.1.6 Scan to E-Mail Configuration Screen Error Messages

This section explains the Scan to E-Mail Configuration screen error messages, along with possible causes and remedies. For more information on the remedies, see "Configuring Scan to E-Mail Settings," on p. 93.

Message	Cause	Remedy
'To' and 'Address Book' are disabled and no default value is specified for 'To' field.	The [To] and [Address Book] check boxes are selected, the [To] text box is blank, and the [Self] check box is not selected.	Perform any of the following: • Clear the check mark from either the [To] or [Address Book] check box, or clear the check marks from both the [To] and [Address Book] check boxes. • Enter a default value in the [To] text box. • Select the [Self] check box.

Message	Cause	Remedy
Default value for 'Subject' field cannot be empty if the field is disabled and required.	The [Subject] check box is selected, the [Subject] text box is blank, and the [Required] check box is selected.	Perform any of the following: • Clear the check mark from the [Subject] check box. • Enter a default value in the [Subject] text box. • Clear the check mark from the [Required] check box.
Default value for 'Subject' field is too long. It cannot exceed 255 characters.	The default value in the [Subject] text box exceeds 255 characters.	Make sure the default value in the [Subject] text box does not exceed 255 characters.
Default value for 'Body' field is too long. It cannot exceed 255 characters.	The default value in the [Body] text box exceeds 255 characters.	Make sure the default value in the [Body] text box does not exceed 255 characters.

6.1.7 Scan to Fax Configuration Screen Error Messages

This section explains the Scan to Fax Configuration screen error messages, along with possible causes and remedies. For more information on the remedies, see "Configuring Scan to Fax Settings," on p. 97.

Message	Cause	Remedy
Fax Recipient Template cannot be empty.	The [Fax Recipient Template] text box is blank.	Enter a fax recipient template.
Fax Recipient Template must contain the 'Fax Number' variable.	The value entered in the [Fax Recipient Template] text box does not contain the 'Fax Number' variable '${FAXNUMBER}'.	Add the variable **${FAXNUMBER}** to the fax recipient template.

6.1.8 Scan to Folder Configuration Screen Error Messages

This section explains the Scan to Folder Configuration screen error messages, along with possible causes and remedies. For more information on the remedies, see "Configuring Scan to Folder Settings," on p. 100.

Message	Cause	Remedy
Connection Failed. Could not connect to *x*:42	The connection to the WINS server failed because Authorized Send cannot connect to the WINS server IP, represented by *x*, and the WINS server port 42.	Check the WINS server IP and try again.

Message	Cause	Remedy
Connection Failed. Could not resolve host name: *x*.	The connection to the WINS server failed because Authorized Send cannot resolve the WINS server host name, represented by *x*.	Check the WINS server host name and/or server configuration and try again.

6.1.9 Create/Update Share Name Screen Error Messages

This section explains the Create Share Name and Update Share Name screen error messages, along with possible causes and remedies. For more information on the remedies, see "Creating a Preset Share," on p. 103, and "Editing a Preset Share," on p. 106.

Message	Cause	Remedy
Share Name is missing.	The [Share Name] text box is blank.	Enter a share name.
File Server is missing.	The [File Server] text box is blank.	Enter the DNS name or IP address to send documents.
File path is missing.	The [File Path] text box is blank.	Enter the path of the folder to send documents.
Share name *x* is reserved. Please choose another one.	The share name, represented by *x*, can be one of the following reserved names: • "-Select Share-" • "Home Directory" • "Home Directory (if exists)"	Enter a share name other than a name that is already on the list of reserved names.
Share name *x* exists. Please choose another one.	The share name, represented by *x*, already exists.	Enter a share name that does not already exist.
Connection Failed. Could not connect to *x*:*y*	The connection to the file server failed because Authorized Send cannot connect to the file server IP, represented by *x*, and the file server port, represented by *y* (139 or 445).	Check the file server IP and try again.
Connection Failed. Could not resolve host name: *x*.	The connection to the file server failed because Authorized Send cannot resolve the file server host name, represented by *x*.	Check the file server host name and/or server configuration and try again.

6.1.10 Options Screen Error Messages

This section explains the Options screen error messages, along with possible causes and remedies. For more information on the remedies, see "Configuring Optional Settings," on p. 113.

Message	Cause	Remedy
Configuration Session Timeout cannot be zero.	Zero is entered in the [Configuration Session Timeout (min)] text box.	Enter a numeric value greater than zero for the configuration session timeout.
Configuration Session Timeout cannot exceed 60 minutes.	A number greater than 60 is entered in the [Configuration Session Timeout (min)] text box.	Enter a number less than or equal to 60 for the configuration session timeout.
Configuration Session Timeout has to be a number.	A non-numeric value is entered in the [Configuration Session Timeout (min)] text box.	Enter a numeric value for the configuration session timeout.
Configuration Session Timeout needs to be set.	The [Configuration Session Timeout (min)] text box is blank.	Enter a numeric value for the configuration session timeout.
Configuration Session Timeout needs to be a positive number.	A negative value is entered in the [Configuration Session Timeout (min)] text box.	Enter a positive numeric value between 1 and 60 for the configuration session timeout.
Network Socket Timeout cannot be zero.	Zero is entered in the [Network Socket Timeout (seconds)] text box.	Enter a numeric value greater than zero for the network socket timeout.
Network Socket Timeout needs to be a positive number.	A negative value is entered in the [Network Socket Timeout (seconds)] text box.	Enter a numeric value greater than zero for the network socket timeout.
Network Socket Timeout cannot exceed 30 seconds.	The number entered in the [Network Socket Timeout (seconds)] text box is greater than 30.	Enter a number less than or equal to 30 for the network socket timeout.
Network Socket Timeout has to be a number.	A non-numeric value is entered in the [Network Socket Timeout (seconds)] text box.	Enter a numeric value for the network socket timeout.
Network Socket Timeout needs to be set.	The [Network Socket Timeout (seconds)] text box is blank.	Enter a numeric value for the network socket timeout.
The application display name is too long. Maximum length is 20 characters.	The application display name entered in the [Application Display Name (up to 20 characters)] text box exceeds 20 characters.	Make sure the application display name does not exceed 20 characters.

Message	Cause	Remedy
Application Display Name cannot contain the following characters: ‘*x*’, ‘*y*’, ‘*z*’	The [Application Display Name (up to 20 characters)] text box contains ‘*x*’, ‘*y*’, and ‘*z*’, which represent invalid characters.	Make sure the application display name is using valid characters. See step 2 in “Configuring Optional Settings,” on p. 113.
***Warning!: Due to the size of the Application Display name entered, Application Display Name may cover the Authorized Send tab icon.**	The application display name entered in the [Application Display Name (up to 20 characters)] text box may be covering up the icon on the display tab.	If this result is not desirable, reduce the size of the application display name entered.
***Warning!: Due to the size of the Application Display name entered, Application Display Name may be cut off.**	The application display name entered in the [Application Display Name (up to 20 characters)] text box may get cut off on the display tab.	If this result is not desirable, reduce the size of the application display name entered.

* This denotes a warning message. A warning message will not stop the saving of the configuration data.

6.1.11 Logs Screen Error Messages

This section explains the Logs screen error messages, along with possible causes and remedies. For more information on the remedies, see “Configuring Log Settings,” on p. 117.

Message	Cause	Remedy
Port for Syslog Server *x* must be a number.	The syslog server *x*, where *x* is 1, 2, or 3, has a UDP port whose value is not a numeric value.	Enter a numeric value for the UDP port.
Port for Syslog Server *x* cannot be zero.	The syslog server *x*, where *x* is 1, 2, or 3, has a UDP port whose value is zero.	Enter a numeric value greater than zero for the UDP port.
Port for Syslog Server *x* must be a positive number.	The syslog server *x*, where *x* is 1, 2, or 3, has a UDP port whose value is a negative number.	Enter a numeric value greater than zero for the UDP port.
Unknown host: *server*	An unknown host, represented by *server*, is entered in the [Syslog Server] text box.	Check the host and try again.
At least one Syslog Server must be configured.	The [Enable Syslog] check box is selected, but no syslog servers are configured.	Either configure at least one syslog server or clear the check mark from the [Enable Syslog] check box.

6.1.12 Change Login ID & Password Screen Error Messages

This section explains the Change Login ID and Password screen error messages, along with possible causes and remedies. For more information on the remedies, see "Changing the Login ID and Password," on p. 162.

Message	Cause	Remedy
New Login ID and Confirm New Login ID do not match.	The value entered for the [New Login ID] text box does not match the value entered for the [Confirm New Login ID] text box.	Enter matching values in the [New Login ID] and [Confirm New Login ID] text boxes.
New Password and Confirm New Password do not match.	The value entered for the [New Password] text box does not match the value entered for the [Confirm New Password] text box.	Enter matching values in the [New Password] and [Confirm New Password] text boxes.
No data has been entered.	No data has been entered in any of the text boxes.	Enter values into the desired text boxes.

6.1.13 Brand Configuration Servlet Screen Error Message

This section explains the Brand Configuration servlet screen error message, along with a possible cause and remedy. For more information on the remedy, see "Using the Brand Configuration Tool (Optional)," on p. 124.

Message	Cause	Remedy
ERROR: *x y* Color :: Invalid property value.	The value *x y*, where *x* is the settings area (Banner, Screen, Button, or Special Button), and *y* is the value in the [Background Color] or [Foreground Color] text box, is not in the correct RGB format.	The RGB format accepts numeric values only. Enter the correct numeric values.
Portal Image Path:: Invalid file type.	The value entered in the [Image Path] text box on the Portal Service Logo screen is an invalid file type.	The valid file types are '.jpg', '.jpeg', '.png', and '.gif'. Enter a valid file type for the portal image path.
Banner Image Path:: Invalid file type.	The value entered in the [Image Path] text box on the Banner screen is an invalid file type.	The valid file types are '.jpg', '.jpeg', '.png', and '.gif'. Enter a valid file type for the banner image path.

6.1.14 Authorized Send Configuration Servlet Log On Screen Error Messages

This section explains the Authorized Send Configuration servlet log on screen error messages, along with possible causes and remedies. For more information on the remedies, see “Flow of Configuration Operations,” on p. 35.

Message	Cause	Remedy
Invalid Login ID and/or Password. Please try again.	The [Login ID] or [Password] text box contains an invalid entry.	Enter the correct login ID or password credentials.
The Authorized Send license has expired. Please contact your Canon dealer.	The Authorized Send license has expired.	Update Authorized Send with a valid license. by contacting your local authorized Canon dealer.

6.2 SIGN IN Screen Notification Messages

The SIGN IN screen notification messages are displayed on the SIGN IN screen in the upper-right hand portion of the MEAP device's UI. You will remain at the SIGN IN screen until they are resolved.

6.2.1 General Authentication Notification Messages

This section explains the general authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
User name and password fields cannot be empty	The [User Name] or [Password] text box is blank.	Enter values for the user name and password, and do not leave them blank.
Please contact administrator to configure this device	You are attempting to log on to a MEAP device that has not been configured by a System Administrator.	Configure Authorized Send for the environment via the Configuration servlet.
Server connect error, connection timed out *(host)*	The log on authentication process exceeds the specified value in the [Network Socket Timeout (seconds)] text box on the Options tab of the Configuration servlet. The default setting is '5' seconds.	• Check that the configured servers are active. • Try to ping the servers from the MEAP device. • Increase the network socket timeout in the Configuration servlet.
Check User Name and Password and try again.	• The [User Name] or [Password] text box contain an invalid entry. • If you are using an authentication method other than Kerberos, this error message may be displayed even if you entered a correct user name and password. In this case, the error message is due to another problem unrelated to the correct credentials.	Enter the correct user name or password credentials. If this does not work, contact the System Administrator.

6.2.2 Kerberos Authentication Notification Messages

This section explains the Kerberos authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Kerberos requires username, password, host and domain	The entered user name or password is blank, or the Configuration servlet host or domain value is blank.	Verify and reconfigure the authentication server settings for the appropriate authentication server in the Configuration servlet, and try to log on again.
Kerberos bind failed, no connection to (*host*)	A Kerberos bind is attempted, and an LDAP connection has not been established.	Check your Kerberos configuration.
Kerberos bind failed, ldap ticket to (*hostname*)	A Kerberos session could not be established.	• Check your Kerberos configuration. • Ensure that the configured server's host name is correct.
Kerberos bind failed to host *(host)* hostname (*hostname*)	A Kerberos bind is unsuccessful to the specified host and host name.	Check your Kerberos configuration.
Unable to get LDAP ticket to (*hostname*)	An LDAP ticket to the host name could not be acquired. Kerberos Error Code: KDC_S_PRINCIPAL_UNKNOWN	• Check your Kerberos configuration. • Ensure that the configured server's host name is correct.
Clock skew exceeds maximum tolerance at host (*host*)	The MEAP device clock and KDC server clock are not within the server's specified maximum clock skew tolerance. The default setting for the Windows 2000, Windows 2003, and Windows 2008 servers is '5' minutes. Kerberos Error Code: AP_ERR_SKEW	Verify that the MEAP device clock and configured server's clock are in sync within the server's maximum clock skew tolerance. For more information, see "Synchronizing the Device and Server Time," on p. 142.
Unable to connect to KDC at host (*host*)	A connection to the KDC at the specified host cannot be reached. Kerberos Error Code: UNABLE_TO_CONNECT_KDC	• Check your Kerberos configuration. • Ensure that the configured server is active.
Unable to connect to KDC at domain (*domain*)	Insufficient cross realm privileges are configured for the MEAP device's domain. Kerberos Error Code: KDC_WRONG_REALM	• Check your Kerberos configuration. • Verify the Kerberos cross-realm configuration.

Message	Cause	Remedy
Unknown host (*host*)	The host cannot be resolved.	- Check your Kerberos configuration. - Ensure that the configured server is active.
An unknown Kerberos error has occurred	Any other Kerberos error message that has not been defined as caught has occurred.	Check your Kerberos configuration.

6.2.3 NTLM Authentication Notification Messages

This section explains the NTLM authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
NTLM requires username, password and domain	The entered user name, password, or domain is blank.	Verify and reconfigure the authentication server settings for the appropriate authentication server in the Configuration servlet, and try to log on again.
NTLM bind failed, no connection to (*host*)	A NTLM bind is attempted, and an LDAP connection has not been established.	Check your NTLM configuration.
NTLM bind failed to host (*host*) domain (*domain*)	A NTLM bind is unsuccessful to the specified host and host name.	Check your NTLM configuration.
An unknown NTLM error has occurred	Any other NTLM error message that has not been defined as caught has occurred.	Check your NTLM configuration.

6.2.4 Simple Authentication Notification Messages

This section explains the Simple authentication notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Check Public DN and Public Password and try again	The public DN and public password have been configured in the Configuration servlet, however they are incorrect.	Verify the public DN and public password.
Anonymous binding not accepted by host (*host*)	The server does not allow anonymous binding, and the public DN and public password are not configured in the Configuration servlet.	• Verify that anonymous connections are enabled on the server. • If anonymous connections are required to be disabled, configure the public DN and public password credentials.
Confidentiality Required	The authentication server you are using has a "Require TLS/SSL" option enabled, and Authorized Send is not using SSL for authentication.	• Disable any "Require TLS/SSL" options on the authentication server. • Enable SSL for authentication in Authorized Send. See "Creating an Authentication Server," on p. 49.

6.3 MAIN Screen Notification Messages

The MAIN screen notification messages are displayed on the MAIN screen in the upper-right hand portion of the MEAP device's UI. If an error has occurred during the authentication process, it will be displayed here.

6.3.1 LDAP Failure Notification Messages

This section explains the LDAP failure notification messages, along with possible causes and remedies.

These errors will not prevent you from authenticating into Authorized Send. However, [Scan to E-Mail] and [Scan to Fax] will be disabled, and you will only be allowed to use the Scan to Folder function.

Message	Cause	Remedy
Your E-mail was not found, admin limit exceeded.	An LDAP server limit set by an admin authority has been exceeded.	Check your LDAP configuration.
Your E-mail was not found, ambiguous response.	An ambiguous response from the server was received by the client.	Check your LDAP configuration.
Your E-mail was not found, authentication not supported.	The client authentication method is not supported by the server.	• Check your LDAP configuration. • Use a different authentication method.
Your E-mail was not found, server busy.	There are too many connections to the server, and the client must wait.	• Check your LDAP configuration. • Increase the amount of connections allowed by the server. • Try authenticating later.
Your E-mail was not found, confidentiality required.	The session is not protected by a protocol, such as TLS.	• Check your LDAP configuration. • Configure Authorized Send with SSL.
Your E-mail was not found, inappropriate authentication.	During a bind operation, the client is attempting to use an authentication method that the client cannot use correctly.	Check your LDAP configuration.
Your E-mail was not found, insufficient access rights.	The client does not have sufficient rights to perform the requested operation.	Check your LDAP configuration.
Your E-mail was not found, bad attribute.	A bad LDAP object has been specified.	Check your LDAP configuration.

Message	Cause	Remedy
Your E-mail was not found, invalid credentials.	Invalid credentials have been supplied by the client.	Check your LDAP configuration.
Your E-mail was not found, invalid DN syntax.	Invalid DN syntax has been supplied by the client (for example, an invalid search root is entered for the authentication server settings in the Configuration servlet).	• Check your LDAP configuration. • Ensure that the configured search root in the authentication server settings in the Configuration servlet is correct.
Your E-mail was not found, LDAP not supported.	LDAP is not a supported protocol on the server.	Check your LDAP configuration.
Your E-mail was not found, searched partial results.	An LDAP referral was received, but was not followed.	Check your LDAP configuration.
Your E-mail was not found, LDAP timed out.	The LDAP server has timed out.	Check your LDAP configuration.
Your E-mail was not found, no results.	No results were returned by the LDAP server.	Check your LDAP configuration.
Your E-mail was not found, bad object class.	The target object cannot be found.	Check your LDAP configuration.
Your E-mail was not found, could not handle referral.	An LDAP referral was received, however it could not be followed.	Check your LDAP configuration.
Your E-mail was not found, time limit exceeded.	The client has exceeded its operation time limit.	Check your LDAP configuration.
Your E-mail was not found, size limit exceeded.	The client has exceeded its operation size limit	Check your LDAP configuration.
Your E-mail was not found, unknown error (*resultCode*).	An unknown LDAP error was received.	Check your LDAP configuration.

6.3.2 Configuration Notification Message

This section explains the configuration notification message, along with a possible cause and remedy.

Message	Cause	Remedy
Please contact administrator to configure E-Mail Service.	There is a bad configuration.	Configure a valid SMTP server for the appropriate address book server in the Configuration servlet.

6.3.3 Warning Notification Message

This section explains the warning notification message, along with a possible cause and remedy.

Message	Cause	Remedy
Usernames over 20 characters may cause issues with AD.	User names that are longer than 20 characters may cause problems with Active Directory.	Make sure the user name does not exceed 20 characters.

6.4 SCAN TO EMAIL Screen Notification Messages

The SCAN TO EMAIL screen notification messages are displayed on the SCAN TO EMAIL screen in the upper-right hand portion of the MEAP device's UI. As you interact with the application, different types of messages are displayed to notify you of an event.

6.4.1 SCAN TO EMAIL Warning Message

This section explains the SCAN TO EMAIL warning message, along with a possible cause and remedy.

Message	Cause	Remedy
Scanning is disabled because the device is not ready.	The MEAP device is still in the process of sending an e-mail message, and you are attempting to start another scan.	• Wait until the MEAP device has completed the operation in progress. • Restart the MEAP device.

6.4.2 SCAN TO EMAIL Input Request Messages

This section explains the SCAN TO EMAIL input request messages, along with possible causes and remedies.

Message	Cause	Remedy
Please specify at least one recipient.	You tried to scan a document to e-mail, but you have not specified an e-mail address, and the [E-mail CC to self] check box is not selected.	• Specify an e-mail address. • Select the [E-mail CC to self] check box from the [Scan to E-Mail] tab in the Configuration servlet. See "Configuring Scan to E-Mail Settings," on p. 93.
Place a document in the ADF or on the Platen then close the lid.	You have not placed a document in the automatic document feeder or on the platen glass.	Place your document in the automatic document feeder or on the platen glass.
Please input subject. It is required.	The device is ready to scan a document to be e-mailed, you did not specify a subject in the [Subject] text box, and the [Subject] text box is configured as enabled in the Configuration servlet.	You must enter a subject before the device scans and sends your document.
Press the [Scan] button or <Start> key to begin scanning.	The MEAP device is ready to scan, and validation for the SCAN TO EMAIL screen is successful.	Press [Scan] or ⊙ (Start).

Message	Cause	Remedy
Press <Enter> key to validate.	The USB keyboard is in use, and a text box was changed that requires validation.	Press [ENTER] on the USB keyboard.

6.4.3 SCAN TO EMAIL Notification Messages

This section explains the SCAN TO EMAIL notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Checking SMTP Connection…	You are attempting to scan and send a document via SMTP.	If the connection is OK, your document is sent to the specified destination.
Checking SMTP Authentication…	You are attempting to scan and send a document via SMTP, and SMTP authentication is enabled.	You must enter the correct user name and password to gain access to the SMTP server.

6.4.4 SCAN TO EMAIL Error Messages

This section explains the SCAN TO EMAIL error messages, along with possible causes and remedies.

Message	Cause	Remedy
Cannot connect to the SMTP Server.	• Connection to the SMTP server cannot be established. • The connection has timed out from the network socket timeout setting in the Configuration servlet.	Contact the System Administrator to make sure that the SMTP server is connected to the network properly, and is accepting connections.
Cannot Authenticate to SMTP Server; Invalid Credentials.	SMTP authentication is enabled, and the SMTP authentication credentials used are invalid.	• If you are not using public credentials, make sure that you enter the correct SMTP authentication credentials on the SMTP Authentication Password pop-up screen. • If you are using public credentials, contact the System Administrator to verify the public credentials configured in the Configuration servlet. See "Configuring the E-Mail Service Settings," on p. 65.

6.5 SCAN TO FAX Screen Notification Messages

The SCAN TO FAX screen notification messages are displayed on the SCAN TO FAX screen in the upper-right hand portion of the MEAP device's UI. As you interact with the application, different types of messages are displayed notifying you of an event.

6.5.1 SCAN TO FAX Warning Message

This section explains the SCAN TO FAX warning message, along with a possible cause and remedy.

Message	Cause	Remedy
Scanning is disabled because the device is not ready.	The MEAP device is still in the process of sending a fax, and you are attempting to start another scan.	• Wait until the MEAP device has completed the operation in progress. • Restart the MEAP device.

6.5.2 SCAN TO FAX Input Request Messages

This section explains the SCAN TO FAX input request messages, along with possible causes and remedies.

Message	Cause	Remedy
Please specify at least one fax number.	You tried to scan a fax document, but you have not specified a fax number.	Specify a fax number.
Place a document in the ADF or on the Platen then close the lid.	You have not placed a document in the automatic document feeder or on the platen glass.	Place your document in the automatic document feeder or on the platen glass.
Press the [Scan] button or <Start> key to begin scanning.	The MEAP device is ready to scan, and validation for the SCAN TO FAX screen is successful.	Press [Scan] or ⊙ (Start).
Press <Enter> key to validate.	The USB keyboard is in use, and a text box was changed that requires validation.	Press [ENTER] on the USB keyboard.

6.5.3 SCAN TO FAX Notification Messages

This section explains the SCAN TO FAX notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Checking SMTP Connection…	You are attempting to scan and send a document via SMTP.	If the connection is OK, your document is sent to the specified destination.
Checking SMTP Authentication…	You are attempting to scan and send a document via SMTP, and SMTP authentication is enabled.	You must enter the correct user name and password to gain access to the SMTP server.

6.5.4 SCAN TO FAX Error Messages

This section explains the SCAN TO FAX error messages, along with possible causes and remedies.

Message	Cause	Remedy
Cannot connect to the SMTP Server.	• Connection to the SMTP server cannot be established. • The connection has timed out from the network socket timeout setting in the Configuration servlet.	Contact the System Administrator to make sure that the SMTP server is connected to the network properly, and is accepting connections.
Cannot Authenticate to SMTP Server; Invalid Credentials.	SMTP authentication is enabled, and the SMTP authentication credentials used are invalid.	• If you are not using public credentials, make sure that you enter the correct SMTP authentication credentials on the SMTP Authentication Password pop-up screen. • If you are using public credentials, contact the System Administrator to verify the public credentials configured in the Configuration servlet. See "Configuring Scan to Fax Settings," on p. 97.

6.6 SCAN TO FOLDER Screen Notification Messages

The SCAN TO FOLDER screen notification messages are displayed on the SCAN TO FOLDER screen in the upper-right hand portion of the MEAP device's UI. As you interact with the application, different types of messages are displayed notifying you of an event.

6.6.1 SCAN TO FOLDER Warning Message

This section explains the SCAN TO FOLDER warning message, along with a possible cause and remedy.

Message	Cause	Remedy
Scanning is disabled because the device is not ready.	The MEAP device is still in the process of sending a document to a shared folder, and you are attempting to start another scan.	• Wait until the MEAP device has completed the operation in progress. • Restart the MEAP device.

6.6.2 SCAN TO FOLDER Input Request Messages

This section explains the SCAN TO FOLDER input request messages, along with possible causes and remedies.

Message	Cause	Remedy
Select a Preset Share or enter a File Server and File Path.	You have a document in the automatic document feeder or on the platen glass, and you have not selected a preset share or entered a file server and file path.	Select a preset share, or enter a file server and file path.
Place a document in the ADF or on the Platen then close the lid.	You have not placed a document in the automatic document feeder or on the platen glass.	Place your document in the automatic document feeder or on the platen glass.
Press the [Scan] button or <Start> key to begin scanning.	The MEAP device is ready to scan the document to the share, and validation for the SCAN TO FOLDER screen is successful.	Press [Scan] or ⊙ (Start).
Press <Enter> key to validate.	The USB keyboard is in use, and a text box was changed that requires validation.	Press [ENTER] on the USB keyboard.

6.6.3 SCAN TO FOLDER Notification Messages

This section explains the SCAN TO FOLDER notification messages, along with possible causes and remedies.

Message	Cause	Remedy
Checking access to [*share*] share…	The MEAP device is attempting to acquire sufficient read privileges.	Not applicable.
Validating File Server and File Path…	The MEAP device is validating correct formatting of the file server and file path.	Not applicable.

6.6.4 SCAN TO FOLDER Error Messages

This section explains the SCAN TO FOLDER error messages, along with possible causes and remedies.

Message	Cause	Remedy
Specified share is inaccessible. Please enter or select another.	The MEAP device cannot acquire sufficient read privileges to the specified file path on the specified file server.	Verify that the share exists and that sufficient privileges have been configured.
Home Directory is not configured. Contact administrator.	The [Scan to Home Directory/Preselected Share only] check box is selected in the Configuration servlet, and the user has no Home Directory configured in Active Directory.	• Verify that the user has a Home Directory configured in Active Directory, or • Clear the check mark from the [Scan to Home Directory/Preselected Share only] check box.
No share is pre-selected. Contact administrator.	The [Scan to Home Directory/Preselected Share only] check box is selected in the Configuration servlet, and no preselected share is selected from the Preselected Share drop-down list.	• Select or configure a preselected share in the Configuration servlet, or • Clear the check mark from the [Scan to Home Directory/Preselected Share only] check box.
No share can be selected. Contact administrator.	The [File Server/Path] and [Browse] check boxes in the <Disabled> column are selected in the Configuration servlet, and no preset shares have been created.	• Create a preset share in the Configuration servlet, or • Clear the check marks from the [File Server/Path] and [Browse] check boxes in the <Disabled> column. See “Configuring Scan to Folder Settings,” on p. 100.